INTERFERENCE DESIGN IN WIRELESS COMMUNICATION SYSTEMS

A Dissertation
Presented to
The Academic Faculty

by

Andrew D. Harper

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
May 2016

INTERFERENCE DESIGN IN WIRELESS COMMUNICATION SYSTEMS

Approved by:

Professor Xiaoli Ma, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Robert J. Baxley
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor John R. Barry
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Thomas D. Morley
School of Mathematics
Georgia Institute of Technology

Professor Aaron D. Lanterman
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: February 5, 2016

ACKNOWLEDGEMENTS

Throughout my graduate studies at Georgia Tech, I have had the distinct privilege of working with numerous people of great and deserving remark. These are people whose intellectual capacity, diligence, and creativity have both inspired and challenged me continuously, and whose achievement and prowess I can only hope to emulate someday. Specially, I would like to thank the core faculty who have guided my research: Dr. Robert J. Baxley, my advisor Prof. Xiaoli Ma, and Prof. Guotong Zhou. My success has in large part been on account of these three individuals, their unwavering support and guidance, their tough questions, their wonderful and unique humor, and at times also their brutal honesty. I am incredibly grateful and forever thankful to have had the opportunity to work closely with faculty of such incredible caliber. I also would like to give special thanks to the remaining members of my SSPARC research team, Dr. Jeremy Reed, Prof. Aaron Lanterman, and Prof. John Barry, Dr. Jonathan Odom, and Dr. Ricky Causey, for their advice and guidance on the project, and for serving as committee members on my thesis. Acknowledgment is due also to DARPA for the financial support of the SSPARC research. I would like to extend thanks as well to my entire research group, and in particular to Prof. Gee-Kung Chang for always providing a unique perspective in seminar. Thanks also to the final thesis committee member, Prof. Thomas Morley. Last, but not least, I would like to thank my family, whose unconditional love and support since the beginning has enabled my success.

Contents

List of Tables

List of Figures

SUMMARY

Interference in wireless communication systems is generally thought of as being produced by an outside, uncontrolled source. With this philosophy, interference must be accounted for and its detrimental effects mitigated. However, there are also cases where interference can be leveraged during system design for its own purpose. This thesis discusses tools for interference design, and proposes new methods for using intentional interference in wireless communications. First, we introduce two tools that can be used in system design. We then present two examples of methods of interference design in wireless communication systems.

Modeling interference in wireless communications can add greatly to the complexity, both analytically and computationally. Useful approximations in interference modeling, are therefore of great interest. The tools we describe both capitalize on effective approximations to reduce complexity, while still yielding accurate solutions. The first tool we present is an approximation of an ad-hoc mesh network of interference nodes. With this model, we show how jamming can be used to minimize the probability that a malicious message is able to travel through a mesh-network of radio nodes.

The second tool we present is an approximation model of a multi-antenna wiretap channel in which noise-like interference is used to generate secrecy. For the multi-antenna wiretap channel, simply finding the maximum achievable secure communication rate often involves a multidimensional brute-force optimization via Monte Carlo simulation. We derive an approximation of the channel using random-matrix theory and asymptotic (in the number of antennas) analysis. We show that our approximation greatly reduces complexity, and is accurate even for finite and reasonable

numbers of antennas.

In the second half of the dissertation, we introduce two methods of interference design. Incorporating interference in the design phase of system modeling can allow for low-complexity analysis. Additionally, intentional interference can sometimes increase secure communication rates and save power. The first method we present is the joint design of a radar-communication system. If both systems fully cooperate, then both systems can eliminate harmful interference from the other system. Moreover, processing redundancies between systems can be eliminated.

Finally, we examine a new method for securing wireless communications. Our proposed technique combines two previously studied secrecy methods: key generation, and artificial noise. We show that the combined use of keys and interference can increase the achievable secure communication rate by leveraging the noise-like property of key-encrypted symbols. Our results demonstrate that the new method presented saves power for a given secrecy rate when compared to the original artificial noise approach. Since both key generation and artificial noise require channel knowledge at the transmitter, we examine both the ideal error free case and the case where channel estimation results in error of a known variance.

Chapter I

INTRODUCTION

Wireless communication systems are constructed for the transmission of information from one point in space to another without the need for a wireline connection. The effectiveness of any communication system is grounded in two metrics: the *rate* at which information is transmitted, and the *reliability* with which the received information can be understood. Combining these two metrics yields the notion of channel *capacity*, or the maximum rate at which information encoded and sent by the transmitter can be reliably decoded by the receiver. In the simplest model, the rate at which information can be transmitted reliably through a wireless channel is limited only by noise. This yields the canonical model for communication

$$\mathbf{y} = \mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{x}$ is the transmitted signal vector, $\mathbf{n}$ is the noise corrupting the transmitted information, and $\mathbf{y}$ is the received signal vector. With the simple models in (1), it is easy to see that how much information we can extract from $\mathbf{y}$ depends on at least two factors: first, how the noise corrupts the information, and second, how we design our input vector $\mathbf{x}$.

We may even generalize the model further to allow for modeling effects of the environment between transmitter and receiver, as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{2}$$

where $\mathbf{H}$ is a matrix representing the wireless channel. Since both the transmitted information symbols and the noise are random, we can only analyze the effect of noise

on the desired signal through statistical properties. Therefore, modeling the distributions of $\mathbf{x}$ and $\mathbf{n}$ is critical to analyzing the performance of the communication system. In contrast, the channel $\mathbf{H}$ may be random or deterministic. For random channels, the distribution influences the system performance; for deterministic channels, how much information about the channel is known *a priori* at the transmitter and receiver will determine the capacity. The general linear model in (2) has been extensively studied. When $\mathbf{n}$ is Gaussian and white, analysis is straightforward and the capacity is easily found in closed form. In general, it is possible to derive analytical expressions for most (interesting) special cases of $\mathbf{H}, \mathbf{x}$ and $\mathbf{n}$.

Noise-limited communication is convenient for analysis. However, in many cases, capacity is limited not only by noise, but also by interference. Interference is measured at the receiver, since it is at the receiver that the information must be extracted from any interference present, and is generally characterized in ways fundamentally different from noise. It is common to characterize receiver noise is modeled as a Gaussian white random process. This denotes that the power spectrum of the noise is constant across all frequencies (of interest), or equivalently that the noise signal is correlated with itself only at a delay of zero. Interference, on the other hand, is generally considered to contain some non-random structure; in fact, this non-random structure not only allows but *necessitates* that it be considered separately from noise. Frequency content of interference is generally restricted to a finite bandwidth, and an interference signal will have a nonzero autocorrelation over a range of nonzero delays.

We can generalize the linear model in (2) to include the effects of interference. If we assume that there are K sources of interference, the model becomes

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \sum_{k=1}^{K} \mathbf{H}_k \mathbf{x}_k + \mathbf{n}, , \tag{3}$$

where $\mathbf{H}_k$ is the channel between the receiver and the k^{th} interferer, and $\mathbf{x}_k$ is the transmitted signal of the k^{th} interferer. Note that the dimensionality of each interferer

may differ from that of the transmitter. Without loss of generality[1], assume that the vector model in (3) represents a wireless communication system using N transmit antennas and M receive antennas and thus $\mathbf{H}$ is of dimension $M \times N$. The k^{th} interferer uses M_i antennas and the k^{th} interference channel is of dimension $M_i \times N$. If the interference originates from a friendly or cooperative source (e.g., other users in the same network), then it might be that $M_k = M$ for all k, or at least we might assume that the M_k are known at the receiver. If, on the other hand, the interference originates from an unknown (or perhaps even adversarial) source, then it is possible that $M_k \neq M$ for *any* k, and likely that the different M_k would be unknown at the receiver.

The dimensionality of interference channels is just one of many considerations. To create an effective model, it is necessary to also have knowledge of (or estimate) other parameters, such as the interference power, interference channel coefficients, and the space-time-frequency structure of the interfering signals. It is clear that the general interference problem can quickly grow exceedingly complex. In fact, the degrees of freedom in the general interference channel modeled in (3) are often too great to yield analytical solutions. This is evidenced by the fact that even seemingly simple interference-channel problems require highly complex and involved solutions. For example, the capacity of the 2×2 interference channel (i.e., two transmitters and two receivers) is still an open problem today, despite more than three decades of research [19].

As the wireless spectrum grows increasingly crowded, the issue of interference from both known and unknown sources will become ever more prominent. Interference is commonly from an outside source, and thus is something to be accounted for, rather than controlled by, the system designers. When interference from an unknown source

[1]In addition to spatial arrays of multiple antennas, the matrix-vector system descriptions in (2) and (3) also commonly represent blocks of symbols gathered over an interval in time or frequency.

is present, there are three main strategies [8]. First, if interference is weak compared to the desired signal, the structure of the interfering signal can be ignored and it can simply be treated as additional Gaussian noise. The effective noise $\tilde{\mathbf{n}}$ and resulting weak interference received signal $\mathbf{y}^{(\mathrm{WI})}$ are then modeled as

$$\tilde{\mathbf{n}} = \sum_{k=1}^{K} \mathbf{H}_k \mathbf{x}_k + \mathbf{n} \tag{4}$$

$$\mathbf{y}^{(\mathrm{WI})} = \mathbf{H}\mathbf{x} + \tilde{\mathbf{n}}. \tag{5}$$

If the strength of the interfering signal is on approximately the same order as the desired signal, the best hope is to orthogonalize the desired signal in either space, time or frequency. Orthogonality ensures the complete separability between signals; desired received signal $\mathbf{y}^{(\mathrm{D})}$ and the interfering received signal $\mathbf{y}^{(\mathrm{I})}$ are then modeled as

$$\mathbf{y}^{(\mathrm{D})} = \mathbf{H}\mathbf{x} + \mathbf{n} \tag{6}$$

$$\mathbf{y}^{(\mathrm{I})} = \sum_{k=1}^{K} \mathbf{H}_k \mathbf{x}_k + \mathbf{n}', \tag{7}$$

where $\mathbf{n}'$ is a new noise term corresponding to the orthogonal space of the interference. Complete separability is in one sense ideal, since the interfering signal can simply be discarded. However, orthogonalization requires either moving to a new location, changing frequencies, or waiting until the interference is no longer present. These options are clearly not desirable, and many scenarios are not even possible. Finally, when interference is strong compared to the desired signal, the best strategy is to decode the interfering signals and remove them. If we define the effect of the k^{th} interferer as $\mathbf{v}_k = \mathbf{H}_k \mathbf{x}_k$, and the receiver's estimate of the k^{th} interference signal as $\hat{\mathbf{v}}_k$, then the strong interference received signal $\mathbf{y}^{(\mathrm{SI})}$ is modeled as

$$\mathbf{y}^{(\mathrm{SI})} = \mathbf{y} - \sum_{k=1}^{K} \hat{\mathbf{v}}_k, \tag{8}$$

where $\mathbf{y}$ is again defined as in (3). Instead of jointly decoding the interfering signals as in (8), it is in practice often more successful to decode successively in order of strength, starting with the strongest, and subtract the single interference estimate before estimating the next strongest. In contrast to the weak-interference approach, decoding the interference capitalizes on the structure present in the interference signal. However, this requires additional knowledge about the interference. For instance, to decode the interference with arbitrarily small probability of error, it may be necessary to have *a priori* knowledge of the codebook with which interference is encoded.

The word "interference" itself generally carries negative connotations. But interference can also be a boon. Figure 1 shows an example of how interference design could be broken down into specific approaches. Though not exhaustive, this diagram is instrumental in comparing the topics covered in this thesis. The traditional pessimistic view of interference is located at the far left of the figure. However, interference design can also be leveraged at the design phase of a communication system to cause a desired effect, either within or outside of the communication network. Examples include intentionally interrupting or corrupting communication, lowering decoding complexity, maximizing throughput, or ensuring privacy.

Crowding of the wireless spectrum will also inevitably drive new approaches to resource sharing between cooperative systems that previously were designed and operated independently. If two systems that compete for resources instead decide to cooperate and share resources,it is possible that both systems can benefit by eliminating harmful interference and minimizing redundancies between them. With full cooperation between systems, it is tempting to immediately incorporate orthogonalization as in (6)-(7), since that allows each system to operate independently. However, even when the interference comes from a friendly or cooperative source, orthogonalization is, in general, a *suboptimal* solution. For example, strictly orthogonal communication systems do not exhaust all degrees of freedom available in the signal space,

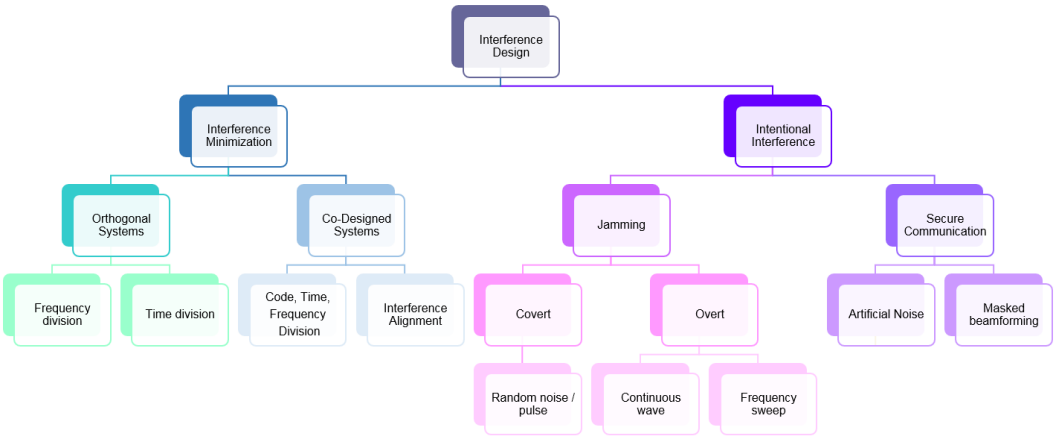


Figure 1: Example interference design tree diagram.

and therefore do not yield rate-optimal solutions. Instead, designing interference to *align* into a specific subspace of the total signal allows full use of degrees of freedom [8]. This illustrates the fact that clever design of interference can actually improve performance.

1.1 Thesis Contributions

Motivated by the inherent complexity of interference in wireless systems and the drive to design interference for specific goals, in this thesis, we describe tools for intentional interference design, and propose beneficial interference methods for wireless communication systems. Here we are concerned with interference at the *physical* layer; we define interference as pertaining to the transmission, propagation, reception, and/or decoding of the wireless signal. The specific contributions of this thesis are as follows.

1. **Tools for Interference System Analysis**

   (a) **Power expenditure in interference networks.** The most familiar form of intentional physical-layer interference is jamming, or flooding the environment with electromagnetic energy to prevent reception of the information signal. Jamming at the physical layer is simple to implement, but

is resource intensive. Power required to transmit a jamming signal continuously is costly. Therefore, when jamming is used, it is desirable to minimize the amount of power necessary to effectively jam a signal. In Chapter 2, we present an approximation model of an ad-hoc mesh network used to interfere with a signal. This approximation model can be used to determine the appropriate system parameters, such as transmission power and number of interfering nodes.

(b) When closed-form expressions for system capacity are not available, we must often resort to simulation to determine the maximum achievable rate. In some interference channels, such as the artificial noise secure communication scheme discussed in Chapter 3, even Monte Carlo simulation can prove burdensome with typical processing hardware currently available. In such a case, an approximation method is needed. We present such an approximation method based on the theory of random matrices, and show that it speeds evaluation by many orders of magnitude.

2. **Methods of Interference Design**

(a) **Codesign of a joint communication-radar system.** In an environment in which cooperative radar and communication systems are co-located and operating simultaneously in the same frequency band, for example, it is possible to design both systems jointly to mitigate interference. Cooperating and sharing resources effectively potentially avoids cross-system interference known to degrade performance of both systems and enables simple linear processing. In Chapter 4, we show the performance of such a joint system with interference eliminated in the design phase.

(b) **Reduced power and increased secure communication rate.** Though constrained interference is likely to be substantially different than noise,

interference that is freely designable may not be. For example, interference can be designed to mimic the properties of white noise, and thereby leverage its random properties. In Chapter 5, we present a novel method of securing wireless communication that leverages noise-like properties of encrypted interference to lower power expenditure and increase achievable secure communication rates.

Chapter II

LINK PROBABILITY IN AD-HOC MESH NETWORKS

Signal jamming is probably the most familiar use of intentional interference in wireless communications. A signal is jammed when interference from an outside source saturates the low-noise amplifier in the hardware of the receiver. This prevents proper amplification of the desired signal, and therefore the desired signal cannot be recovered. Jamming is simple to implement and broadly effective; all that is required is a high level of transmitted energy in the same signal space as the target receiver. However, high power transmission is at the very least quite costly, and in some cases not feasible. In this chapter, we study the use of low-power resource-constrained radios for jamming. In particular, we examine how, using an approximation network of randomly placed power-limited radios, we can use the probability of any one radio establishing a link to prevent a message from traversing the space. We conclude this chapter by showing how this model can be used in interference design in selecting between random radio dispersement and a rectangular grid placement.

2.1 Introduction

The emergence of a number of affordable AHMN devices has broadened both availability and appeal of wireless mesh networking. As is often the case with wireless devices, it also introduced a new set of concerns about interference in shared bandwidths. Many AHMN devices offer sensors that facilitate gathering data from the environment of the sensor network. These devices are generally inexpensive, and operational straight out of the box, and are intended for varied applications such as monitoring the structural health of a bridge [10] or home-based health monitoring systems [61]. The versatility, availability, and user-friendliness of AHMN devices

also introduces the possibility of their use for malicious purposes, such as remote explosive detonation. In such applications, the ability to interfere with the network transmission, and subsequently the ability of the network to withstand attempts at interference, are of great interest.

Recent works have addressed avoidance of interference from devices with similar hardware to that of the network, thereby limiting the possibilities of transmitted interference. In such cases, the AHMN may employ a variety of options to avoid transmission concurrent with the interferer in time or in frequency. However, interfering devices may not have similar constraints on bandwidth, waveform type, power output or range of transmission. The Universal Software Radio Peripheral (USRP) is one of a recent class of software defined radios (SDRs) that offer extremely flexible programming– allowing for wideband interference, specifically targeted waveforms, and more versatile output power. This flexibility enables a new class of adversarial interference governed primarily by minimizing link probability in the AHMN.

In this chapter we establish an analytical framework for predicting the probability that an in-network link exists in the presence of multiple interferers. Through analysis, we find the probability that a given pairwise link exists in an AHMN with randomly placed relay nodes. Then, by modeling the successive relay selections as a Markov process, successful message reception is indicated by the stationary distribution of the Markov process.

The organization of this chapter is as follows: Section 2 discusses previous works that address the interference different contexts of wireless network communication. In Section 3, we define the model used in our analysis. In Section 4, we derive in-network link probabilities as a function of communication and interference transmission radii. We validate our model through Monte-Carlo simulations, and give an example of its use in Section 5. We finish in Section 6 with conclusions and possible directions for future work.

2.2 Background and Related Work

Device designers generally equip AHMN devices with a self-interference avoidance algorithm to prevent intra-network interference. Many devices with advanced programming support may have these algorithms disabled, allowing the possibility of using identical hardware to interfere with communication. Previous works have investigated interference that might be presented using 802.15.4 devices. Woods *et al.* [96] propose a sequence of jamming attacks and counter-jamming responses, where the communicator and jammer successively adapt to the actions of the other. This research is illustrative of the constantly oscillating nature typical of a zero sum game– the attacking strategy is valid only until a defensive maneuver defeats it. They model interference in a point to point format with three nodes (sender, receiver and interferer), and quantify the performance experimentally by measuring the packet delivery ratio (PDR). The authors claim that their methods yield an 88% PDR, and that the interferer is left no option that will more effectively denigrate transmission. However, interference generated by a versatile SDR would not be so constrained in attacking strategy.

Other previous works have also addressed channel access issues. Stamatiou & Proakis [79] use an AHMN model similar to ours, and assess network throughput as a function of self-interference avoidance strategy. They examine the theoretical performance metrics for various multiple access (MA) scheme in avoiding self-interference in multiple-input multiple-output (MIMO) systems. Li *et al.* [43] also use a randomly placed network model similar to the one used in this chapter, and investigate optimal jamming attacks in wireless sensor networks where the jamming parameters are controllable. Their work differs from ours in that it focuses on modeling the detection of interference, which in our model is unimportant. They also assume symmetrical links between communicating nodes, a simplification which cannot be adopted in studying directional communication. Khattab *et al.* [40] consider channel hopping to avoid

interference, and evaluate the advantages of reactive (in response to detected jamming activity) versus random (without regard to channel activity) hopping. They find proactive hopping best for nodes with a single radio, and reactive best for nodes with multiple radios. However, wideband interference might alter these results.

Many previous works have considered the optimal physical layer interference strategies. Martin & McAdam [52] prove that for an average power constrained Gaussian noise interferer, pulsed interference performs optimally. They show that short pulses of higher-intensity interference are more effective per unit power than continuous lower-intensity interference in producing bit errors at the receiver. Optimal transmitter/interferer strategies have also been analyzed from information theoretic viewpoint for systems with various constraints. Wang and Giannakis [92] analyze a two-hop relay scenario. In the case of no fading, they show that the best strategy is to interfere with a linear combination of the transmitted signal and Gaussian noise. In a fading channel, though, they prove that a Gaussian noise interference strategy is optimal even with perfect knowledge of the transmitted signal. Kashyap *et al.* [37] consider interference on a MIMO Gaussian Rayleigh-fading channel, and show that in such systems knowledge of the transmitted signal does not increase effectiveness of interference.

The wide body of previous research has addressed both medium-access and physical layer point-to-point interference. However, models of analysis of physical layer interference from multiple sources are not as mature. We present a here simple model which has the potential for extension to more specific and complex applications in the future. Our model is also unique in that we analyze the pairwise link probability and its effect of transmitting a single message, rather than assessing network throughput averaged over time. and use a Markov model to gage expected effectiveness. We consider a network of single-radio, single-input single-output nodes in the presence of multiple interferers, and assume an arbitrary interference strategy such

that transmitted signals will be met with interference at all instances.

2.3 Model and Definitions

We are interested in the effects of non-cooperative interference on the performance of the network. Hence, we assume that a self-interference avoidance algorithm is implemented that makes the probability of self-interference negligible. As an example, to avoid multiple access interference within the network, 802.15.4 [30] uses carrier sense multiple access with collision avoidance (CSMA-CA) to sense channel activity before transmitting.

2.3.1 Physical Model

The transmission space S is modeled as a square of area $|S| = w^2$, populated with up to N communicating relay nodes $n \in \{1, \ldots, N\}$. The AHMN node coordinates are selected randomly from a uniform distribution across the space. A sending node c_s is positioned randomly along the left edge of the space, and a receiving node c_r randomly along the right edge. The goal of the mesh network nodes is to relay a single message from sender to receiver through h hops across the network. All AHMN nodes are assumed to have both sending and receiving capabilities, and are constrained to have identical power output. We denote the availability of a link from c_i to c_j as $c_i \rightarrow c_j$, and a reciprocal link as $c_i \leftrightarrow c_j$.

The transmission space is then populated with up to M interfering nodes m, $m \in \{1, \ldots, M\}$ whose goal it is to prevent the transmission of the message from c_s to c_r. The interference node coordinates are selected randomly from a uniform distribution across S. We denote the interference from d_i to c_i as $d_i \rightarrow c_i$, and lack of interference from d_i to c_i as $d_i \nrightarrow c_i$. Figure 2 shows a graphic example of one possible rendering of the model. The sending node is located on the left edge of the image, and the receiving node on the right. Black squares with white borders represent AHMN nodes. Available links between nodes are shown as arrows. White

squares with black borders represent interfering nodes. The grayscale contour shows the sum effect of all interfering nodes at various power levels.

Note that, for any given realization, the existence of a reciprocal link between c_i and c_j cannot be assumed due to asymmetries in relation to interfering nodes. That is, in a symmetrical link network,

$$\begin{aligned}\Pr(c_i \to c_j | M = 0) &= \Pr(c_i \leftarrow c_j | M = 0) \\ &= \Pr(c_j \leftrightarrow c_i | M = 0),\end{aligned}$$

but in general

$$\begin{aligned}\Pr(c_i \to c_j | M > 0) &\neq \Pr(c_i \leftarrow c_j | M > 0) \\ &\neq \Pr(c_i \leftrightarrow c_j | M > 0).\end{aligned}$$

We assume the self-interference mitigation algorithm (e.g. 802.15.4 CSMA-CA) is effective in preventing packet collision within the communication AHMN, and that all interference arises from interfering nodes. MAC sublayer strategies (channel hopping, packet fragmentation, redundant encoding) for evading intentional interference are omitted, and we focus exclusively on the results of concurrent transmission of communicating nodes and interfering nodes. For simplicity we assume an isotropic radiation pattern and the standard free-space power decay model, as might be used to approximate a level outdoor environment. We note in advance that whether or not our analysis could be applied to a fading channel model remains an open question. Each communication node has an identical maximum radius of transmission $r_{\max}$ determined [78] by its power output through

$$r_{\max} = \left(\frac{P_{\mathrm{t,max}} G}{4\pi P_{\mathrm{r,min}}} \right)^{\frac{1}{2}} \tag{9}$$

where G is an attenuation constant which accounts for non-ideal radiation and antenna reception. As an example, consider an IEEE 802.15.4 system where $P_{\mathrm{t,max}} =$ 0dBm is the maximum power transmission capability, and $P_{\mathrm{r,min}} = -85$dBm is the

minimum power reception necessary to establish a reliable link. The minimum and maximum power requirements are set according to IEEE 802.15.4 specifications, and $G = 1.5 \times 10^{-4}$ is defined to yield a maximum range of 60m.

2.3.2 Relay Model

The ultimate goal of this analysis is to determine whether a message can migrate across an AHMN of relays from a source node to a destination node, denoted by $c_1 \twoheadrightarrow c_N$. Thus we can determine whether the source and destination are connected through the relays by determining whether there exists any fully connected path through the relays that connect the source to the destination.

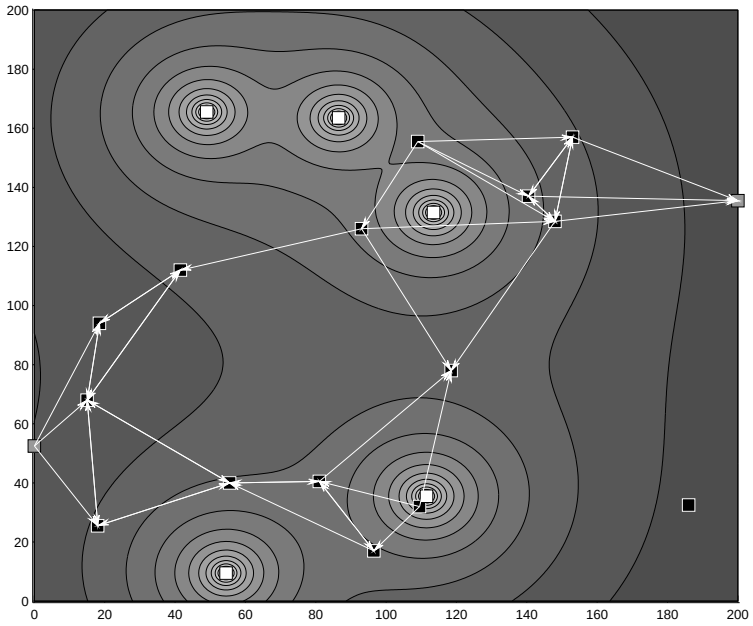
To model this, we assume that each relay broadcasts any received message to any relay in range. Subsequent relays do the same. In this way, all possible path are tested so that if a path through the relays between the source and destination exists, the message will be successfully received.

Analytically, this physical-link relay scheme can be modeled as a Markov process where the probability that the message is successfully received in time step $i+1$ by node $c_j^{(i+1)}$, when sent in time step i from node $c_k^{(i)}$ is conditionally independent of all previous hops given that c_k successfully received the message in time step i. That is,

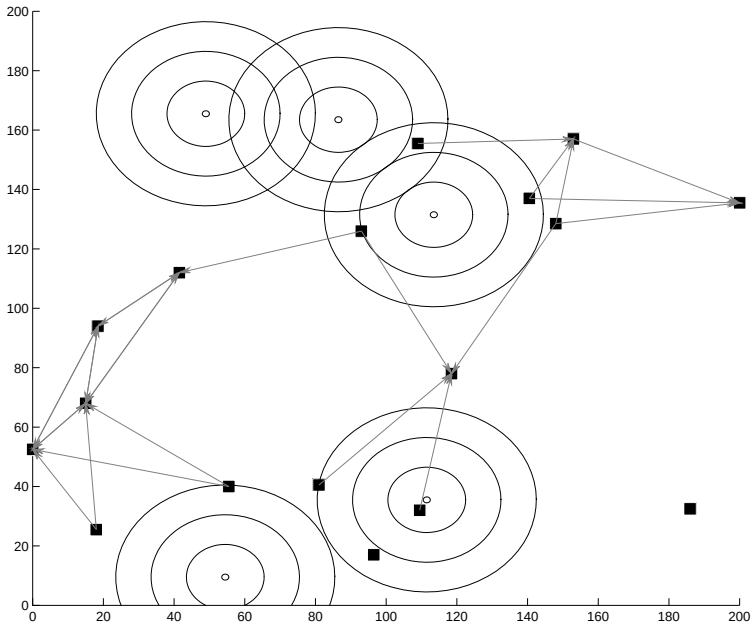
$$\begin{aligned} Pr(c_k^{(i)} \to c_j^{(i+1)} | c_k^{(i)}, c^{(i-1)}, ..., c^{(0)}) \\ &= Pr(c_k^{(i)} \to c_j^{(i+1)} | c_k^{(i)}) \\ &= Pr(c_k \to c_j | c_k) \\ &= [\mathbf{T}]_{k,j}, \end{aligned} \tag{10}$$

where $\mathbf{T} \in \mathbb{R}^{N \times N}$ is the transition matrix.

Form here there are two ways to analyze the network throughput performance. The ergodic view of the network involves assuming that every link has a certain probability of success quantified by $Pr(c_k \to c_j | c_k)$ however small it might be. With



(a) Example network layout.



(b) Approximation network.

Figure 2: (a) Randomly generated network, and (b) its corresponding approximation.

this, the probability of successful transmission after K hops by is given by

$$Pr(c_1 \twoheadrightarrow c_N | K \text{ hops}) = [\mathbf{T}^K]_{1,N}. \tag{11}$$

An example $\mathbf{T}$ is shown in the top left of Fig. 3. In this graphical representation, rows represent senders and columns represent receivers. Each square thus shows the probability of the row node establishing a link with the column node, with black being zero probability and white being probability 1. The nodes are not allowed to transmit to themselves, so the matrix is black on the diagonal with the exception of the receiving node which is white signifying that it is an absorbing state. The gray values represent the estimated average probability of all other links. This model does not account for asymmetries in link probability due to the spatial arrangement of interfering nodes.

The alternative is to assume that the network is made up of connected relays and unconnected relays as illustrated in the bottom three images of Fig. 2. This view provides a better model of the effects of receiver saturation by an interferer. That is, at a certain level of interference power, the low-noise amplifier (LNA) present in any practical transmission system will saturate, making reception by the relay impossible regardless of the signal power.

In this case, the transition matrix $\tilde{\mathbf{T}}$ is a random variable that depends on the realization. The elements of $\tilde{\mathbf{T}}$ are normalized Bernoulli distributed with probability $Pr(c_k \to c_j | c_k)$. That is

$$\Pr([\tilde{\mathbf{T}}]_{k,j} \neq 0) = \Pr(c_k \to c_j | c_k) \tag{12}$$

and

$$\Pr([\tilde{\mathbf{T}}]_{k,j} = 0) = 1 - \Pr(c_k \to c_j | c_k). \tag{13}$$

In this case, the probability of successful transmission after K hops by is given by

$$\Pr(c_1 \twoheadrightarrow c_N | K \text{ hops}) = Pr([\mathbf{T}^K]_{1,N} \neq 0) \tag{14}$$

and the probability of successful transmission at any time is

$$\lim_{K\to\infty} \Pr(c_1 \twoheadrightarrow c_N | K \text{ hops}) = \Pr([\mathbf{T}^K]_{1,N} \neq 0). \tag{15}$$

Three example realizations of $\tilde{\mathbf{T}}$ are shown in Fig. 3. Observe that each realization produces a unique transition matrix, and that link probabilities are no longer dependably reciprocal.

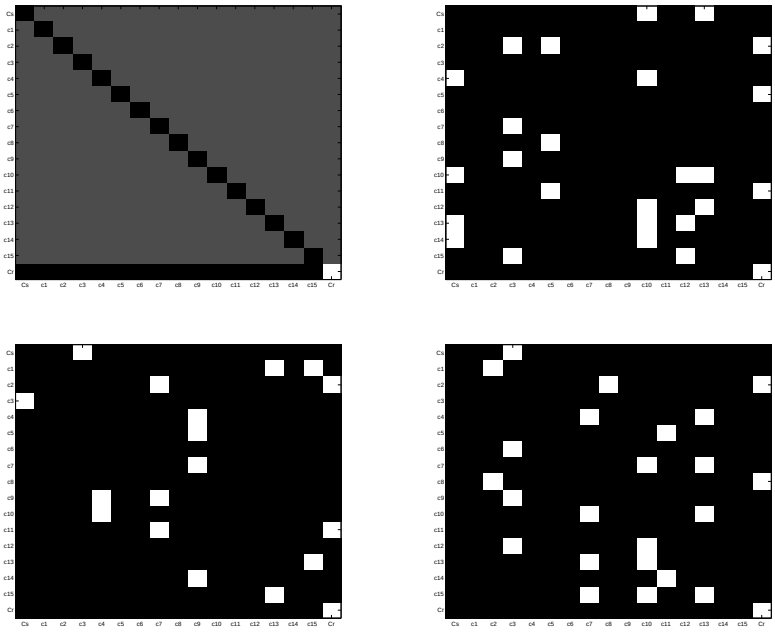


Figure 3: (Top left) Graphical representation of the $\mathbf{T}$ transition matrix. (Top right, bottom row) Three different realizations of the $\tilde{\mathbf{T}}$ transition matrix.

2.4 Link Probabilities

We now derive the probability of link within the AHMN in the presence of multiple interferers.

Theorem 1. *Let S be a square space with side length w. Given an arbitrary number of uniformly distributed communicating nodes c_i, $i \in \{1, 2, \dots\}$ with maximum transmission radius $r_c < w$, the probability of link from the ith to the jth node in the*

absence of interference is

$$Pr(c_i \leftrightarrow c_j | M = 0) = \left(\frac{r_c^4}{2w^4} - \frac{8r_c^3}{3w^3} + \frac{\pi r_c^2}{w^2} \right) \tag{16}$$

Proof. In a square space with side length a, the probability distribution $f_X(x)$ of length X between any two independently and uniformly selected points within the space has been shown [53] to be

$$f_X(x) = \frac{4x}{a^4} \left(\frac{\pi a^2}{2} - 2ax + \frac{x^2}{2} \right), 0 \leq x \leq a. \tag{17}$$

For the space S, we have $a = w$. Since we are interested in analyzing transmission across an AHMN, we assume that the maximum transmission radius is not sufficient to cross the network in a single hop. Thus, $r_c < w$, and the distribution is

$$f_X(x) = \frac{2x^3}{w^4} - \frac{8x^2}{w^3} + \frac{2\pi x}{w^2}, x \leq r_c < w. \tag{18}$$

The probability that the jth node is in range of the ith node then becomes

$$\begin{aligned} \Pr(c_i \leftrightarrow c_j | M = 0) &= \int_0^{r_c} f_X(x) dx \\ &= \frac{r_c^4}{2w^4} - \frac{8r_c^3}{3w^3} + \frac{\pi r_c^2}{w^2}. \end{aligned} \tag{19}$$

□

Using a similar analysis, we arrive at the probability of link from c_s to a node within S as

$$\Pr(c_s \rightarrow c_j | M = 0) = \frac{\pi r_c^2}{2w^2} - \frac{2r_c^3}{3w^3}. \tag{20}$$

Since c_s and c_r are independently and uniformly placed along sides of equal length, $\Pr(c_s \rightarrow c_i | M = 0) = \Pr(c_i \rightarrow c_r | M = 0)$. For the derivation of (20), we again refer to [53] and leave the proof as an exercise for the reader.

Theorem 2. *Let S be a square space with side length w. Given a finite number of uniformly distributed interfering nodes d_i, $i \in \{1, 2, \ldots, M\}$ with maximum transmission radius $r_d < w$, the probability of a point c being free from interference is*

$$Pr(d_1 \ldots d_m \nrightarrow c) = \left(1 - \frac{r_d^4}{2w^4} + \frac{8r_d^3}{3w^3} - \frac{\pi r_d^2}{w^2} \right)^M. \tag{21}$$

Proof. Following the same procedure as Theorem 1, we arrive at the probability that ith node d_i interferes with c as

$$\Pr(d_i \to c) = \frac{r_d^4}{2w^4} - \frac{8r_d^3}{3w^3} + \frac{\pi r_d^2}{a^2}, \tag{22}$$

and thus

$$\Pr(d_i \nrightarrow c) = 1 - \left(\frac{r_d^4}{2w^4} - \frac{8r_d^3}{3w^3} + \frac{\pi r_d^2}{a^2} \right). \tag{23}$$

Since all interfering nodes are independent of one another, we have

$$\begin{aligned} \Pr(d_1 \dots d_m \nrightarrow c) &= \Pr\left(\bigcap_{m=1}^{M} d_m \nrightarrow c \right) \\ &= \prod_{i=1}^{M} \Pr(d_i \nrightarrow c) \\ &= \left(1 - \frac{r_d^4}{2w^4} + \frac{8r_d^3}{3w^3} - \frac{\pi r_d^2}{w^2} \right)^M. \end{aligned} \tag{24}$$

□

Theorem 3. *Let S be a square space with side length w. Given an arbitrary number of uniformly distributed communicating nodes c_i, $i \in \{1, 2, \dots\}$ with maximum transmission radius $r_c < w$, a finite number of uniformly distributed interfering nodes d_i, $i \in \{1, 2, \dots, M\}$ with maximum transmission radius $r_d < w$, the probability of link free from interference from the ith to the jth node is*

$$Pr(c_i \to c_j) = \left(\frac{r_c^4}{2w^4} - \frac{8r_c^3}{3w^3} + \frac{\pi r_c^2}{w^2} \right) \left(1 - \frac{r_d^4}{2w^4} + \frac{8r_d^3}{3w^3} - \frac{\pi r_d^2}{w^2} \right)^M. \tag{25}$$

Proof. The proof follows from the combination of Theorems 3 and 4, and the independence of the communicating and interfering sensor networks. □

2.5 Simulation

To verify Theorem 1, we performed a Monte-Carlo simulation of our AHMN for all transmission radii less than 60m, the maximum radius for an 802.15.4 network. The results are shown in Fig. 4. The top curve shows the theory and simulation

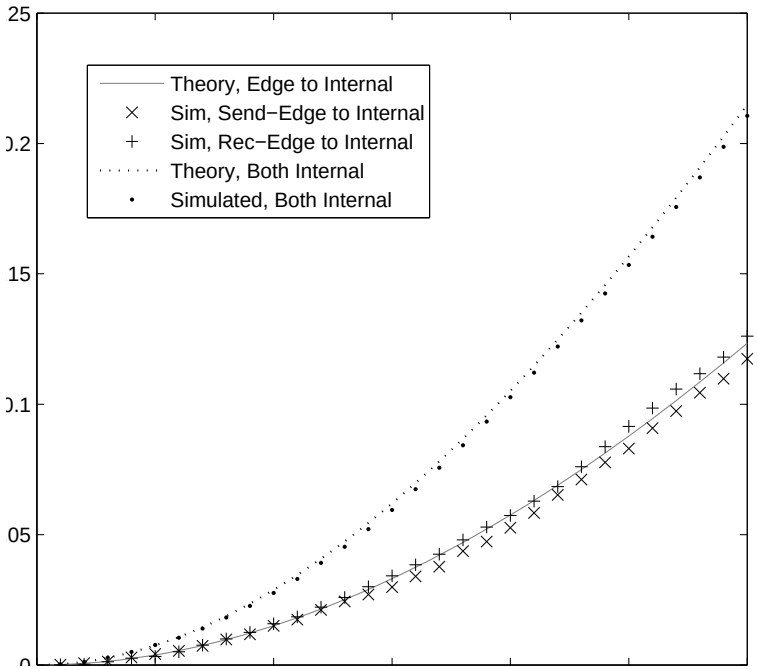


Figure 4: Probability of link in the absence of interference.

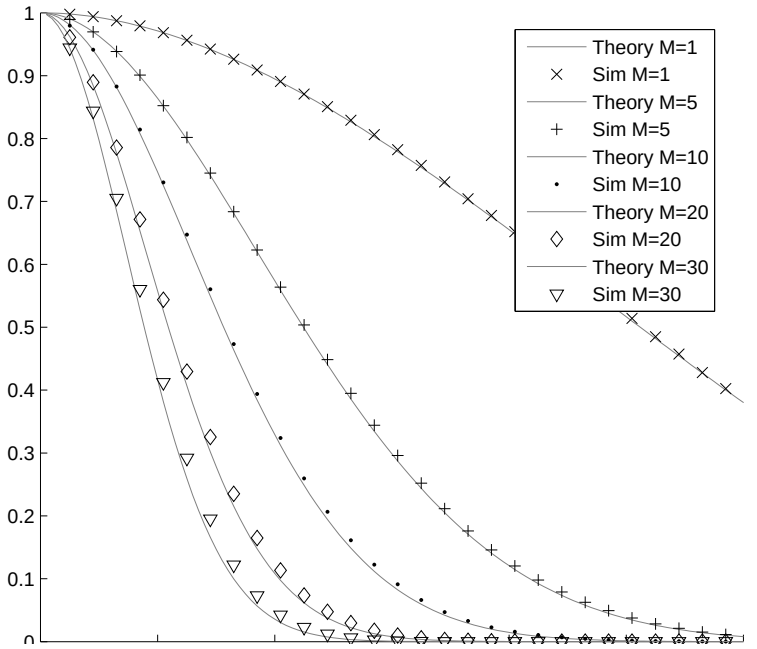


Figure 5: Probability of escaping interference.

comparison for the case where both communicating nodes are within S. The lower curves represent the theory and two simulations for when one node is within S and one is located on an edge, as is the case for c_s and c_r. The probability is lower for links with sending and receiving nodes, since their horizontal component is fixed and thus are out of range more nodes placed on the right side of S. The small offset in the simulated values may be due to quantizing S into a grid of points instead of a considering it a continuous space. We verified Theorem 2 in a similar manner. The results are shown in Fig. 5. The probability of link decreases with each additional interfering node placed in S. However, as the space becomes more saturated, the placing additional interfering nodes begins to show diminishing returns. We now follow with an example of how this modeling of AHMN might be useful in practice.

2.5.1 Example: Effects of Node Density and Spatial Arrangement

In designing a system to interfere with an AHMN, two central considerations are interfering node density and node layout. As an example scenario, consider a situation where the goal is to jam a AHMN with exactly M jammer nodes. To achieve the objective of maximum jamming efficiency, we must first determine should the jamming nodes be spatially organized. We consider two options: place the jammers on a rectangular grid or place the jammers randomly. The former placement is more intuitively appealing and does provide better performance for some values of M. In contrast, random jammer placement may be easier to deploy by, for instance, dropping the jammer node out of a plane.

We simulate this scenario, and keep the number of AHMN nodes constant as we vary the size of the space S and the number of interfering nodes M. Fig. 6 shows Monte-Carlo simulation results for two runs, each with $N = 15$ AHMN relay nodes. In the top figure, S has side length 140m, while in the bottom figure the length is increased to 260m.Two different interfering node layouts are tested: a

randomly assigned layout, and a square grid layout. We assume the interferer has control of node placement, and thus can select the better arrangement once it is known. The graphs trace expected probability of transmission through the network. At low AHMN densities, the performance of the grid and random layouts are similar, and overall probability is reduced.This matches intuition, since in sparser networks the link probability is diminished, and a grid layout of interfering nodes is likely to cover a similar amount of territory as the random layout. As the densities are increased, however, we see the curves begin to differentiate. Now, there are regions where the random placement performs better than the grid layout, and vice versa. If the interferer is more constrained by number of nodes, a grid spacing will more effectively disrupt transmission. However, as interfering nodes increase, likelihood of transmission is depleted more quickly with a random arrangement.

2.6 Discussion

In this chapter we present a closed-form expression for the probability of pairwise AHMN node link in the presence multiple interferes. We then show through Monte-Carlo simulation that a simple binary Markov model accurately approximates these link probabilities. We have also demonstrated an example application for how the model might be useful in AHMN network design. The models presented here are a first step in a novel approach to modeling AHMNs. Though this first model is somewhat simplistic, it nonetheless is able to account for non-reciprocal pairwise link probability. Future iterations could tailor the model to more specific needs and research areas. Possible extensions might include assessing the effects of additive noise, incorporating indoor or urban fading characteristics into the transmission model, and accounting for contour created by summation of interference signals.

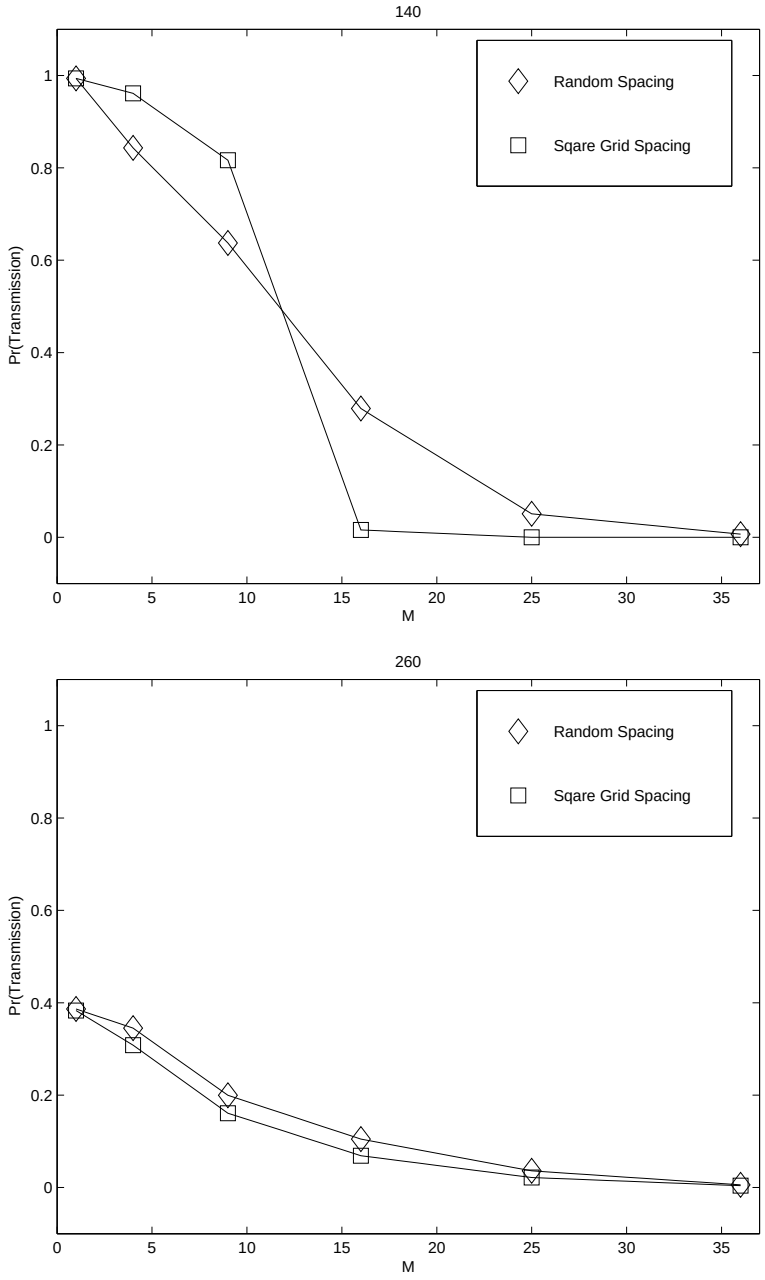


Figure 6: Comparison of random and grid interferer performance for dense (top) and sparse (bottom) realizations.

Chapter III

LARGE-SCALE MIMO APPROXIMATION FOR ARTIFICIAL NOISE

In Chapter 2, we modeled our interference radio transmitters with a simple isotropic radiation. With multi-antenna transmission, it is possible to weight the signals transmitted by each antenna to direct energy more effectively. This enables new possibilities for interference design over the single-antenna case, in particular with regard to secure communication. Given sufficient transmit antennas, signal energy can be directed toward, and interference can be directed away from, the intended receiver. Maximizing achievable secure communication rates with this technique involves optimization over multiple variables, and is in general a non-convex problem. Therefore, researchers often resort to brute-force search for optimum values using Monte Carlo simulation.

Even with standard computational power growing continuously and quickly as it has in recent decades, these optimizations can still prove cumbersome and time consuming as a result of the number of variables involved. Therefore, in this chapter, we present a tool useful in interference design which approximates the interference channel. This approximation uses random matrix theory, and assumes that all parties are equipped with infinite antennas. Although such an assumption seems unreasonable, we show that the approximation remains accurate even for small numbers of antennas. The approximation tool is shown to speed calculation of rates achievable with optimal values by orders of magnitude over Monte Carlo simulation.

3.1 Introduction

In 1975, Aaron Wyner defined the *secrecy capacity* for a three-terminal system with a transmitter, intended receiver, and eavesdropper, called the "wiretap channel". The secrecy capacity is the maximum reliable rate of communication between transmitter and intended receiver, with the eavesdropper unable to glean any information from the message [97]. In a discrete memoryless channel where the eavesdropper's channel is degraded with respect to the main channel (e.g. the eavesdropper channel is noisier), [97] showed that the secrecy capacity is strictly positive. This result is based on wired communication, where it is reasonable to assume that an eavesdropper tapping the line would receive a degraded copy of message arriving at the intended receiver.

The notion of secrecy capacity was extended first to the *broadcast* discrete-memoryless channel in [15], and subsequently generalized to the Gaussian wiretap channel in [42]. The basic results of these works are analogous to the wired case: the secrecy capacity is strictly positive whenever the eavesdropper channel is in some sense "worse" than the main channel. In a wireless communication system, an eavesdropper located further from the transmitter than the intended receiver is likely to have a noisier channel simply by the properties of free-space propagation loss. It was shown in [2, 6] that in rich-scattering multipath channels, the ergodic secrecy capacity is nonzero even when the SNR at the Ex exceeds that at the Rx. However, if the eavesdropper's location is unknown *a priori*, the relative channel quality cannot be guaranteed. However, if the transmitter is equipped with multiple antennas outnumbering the number of antennas at the receiver and eavesdropper, then it is possible to devote a portion of available power to transmitting noise in all directions away from the intended receiver, and thereby artificially degrade the eavesdropper channel regardless of its exact location.

This method of securing communication was first put forth in [21, 22] and is termed

artificial noise (AN) [1]. With accurate channel knowledge at the transmitter, singular-value decomposition (SVD) can be used to transform a general MIMO channel into a set of parallel independent channels. To preclude adding noise to the main channel, message and AN symbols are precoded with right singular vectors corresponding to nonzero and zero singular values, respectively. The transmitter can thus simultaneously transmit message symbols to the intended receiver and direct AN symbols in the direction of any potential eavesdroppers. An eavesdropper's only choice is then to attempt to increase SNR by physically approaching the Tx. However, at high SNR the eavesdropper's gains saturate while those of the main channel continue increasing, thereby guaranteeing a positive secrecy capacity is attainable regardless of the eavesdropper's proximity to the Tx.

Other works have also investigated the AN strategy from a number of different perspectives. Khisti and Wornell [41] first explored the use of AN for the the deterministic multiple-input single-output multiple-eavesdrop (MISOME) wiretap channel, and showed that the AN method yields a rate asymptotically (in power) near secrecy capacity. Zhou and McKay [105] derived closed-form lower bounds for the achievable secrecy rate for the multiple-input single-output single-eavesdrop (MISOSE) fading channel, for the MISOSE channel with multiple single-antenna eavesdroppers operating independently, and for the MISOSE channel with multiple eavesdroppers in collusion, which can be considered equivalent to the MISOME case. Optimal power allocation between the information signal and AN has also been previously studied. For the MISOSE channel with multiple non-colluding eavesdroppers, it is shown in [105] that splitting power equally between information and AN signals yields near-optimal performance; however, as eavesdroppers are allowed to collude, more power

[1] Although [21] uses the term *secrecy capacity* in reference to the maximum secret rate as the artificial noise secrecy capacity, artificial noise is strictly suboptimal and thus cannot achieve the secrecy capacity. Therefore, in this dissertation we use the term secrecy *rate*.

should be devoted to AN as the number of eavesdroppers grows. In [63], power allocation and AN in an orthogonal frequency-division multiplexing (OFDM) system are analyzed, and it is shown that frequency-domain AN is insufficient to guarantee secrecy; rather, a time-domain AN signal must be superimposed.

In [103] a wiretap code is adaptively optimized given a low-rate instantaneous channel state information (CSI) feedback signal from the receiver. Most previous studies of AN assume that, while the exact eavesdropper channel is unknown, the statistics of the eavesdropper are known at the transmitter. In contrast, [58] considers the case where no information about the eavesdropper channel is available, and analyses the achievable secrecy rate using a signal to interference plus noise (SINR) metric. To effectively steer AN and signal into orthogonal spaces, the transmitter is commonly assumed to posses accurate CSI. The effect of imperfect CSI at the transmitter (and subsequent noise leakage into the main channel) is considered in [58, 46, 44]; imperfect CSI at the receiver is considered in [98]. In [69], power allocation is considered from an outage probability perspective for the MISO case.

In [45], the authors generalize the artificial noise framework to allow transmission of AN power into the main channel for the special MISOSE case where the transmitter may have multiple antennas but the intended receiver and the eavesdropper are each equipped with only a single antenna. Their analysis shows that, contrary to intuition, the optimal beamforming matrix does not strictly limit the AN transmitted to the null space of the main channel; rather, modest secrecy gains can be achieved in lower SNR regions where the zero-forcing solution yields zero secrecy capacity. However, as the number of antennas increases, this generalized approach quickly converges to the orthogonal approach of precoding with right singular vectors in [21]. The difference also diminishes, albeit more slowly, with increases in SNR. Since the returns from optimizing as in [45] diminish quickly, and complexity is substantially increased compared to SVD, the orthogonal decomposition method in [21] remains an attractive

approach.

3.1.1 Problem Formulation

Calculating secrecy capacity involves expectation over random channel gains via Monte-Carlo simulation, followed by optimization over both antenna and power allocation variables. The complexity involved with this task makes it unfeasible for resource-constrained or adaptive systems. Moreover, the solution is applicable only for the specific number of antennas at Tx, Rx, and Ex for which it is generated. Comparing a chosen implementation to the maximum achievable involves either generation and storage of large lookup tables or simulation for each tested configuration. Our objective in this chapter is to develop a method of approximating the AN secrecy capacity presented in [21] that:

1. is closed form,
2. is accurate and useful for realistic power levels and numbers of antennas,
3. generalizes the channel model to include arbitrary independent and identically distributed (i.i.d.) channels, and
4. does not weaken security by overestimating the rate at which secret communication is possible.

We show here that an approximation method meeting these criteria is possible by applying large-scale MIMO analysis techniques, and recent results from random matrix theory. A critical estimate is the worst-case eavesdropper capacity; this quantity is an upper bound on the amount of information that an eavesdropper may be able to decode. By reformulating the eavesdropper capacity as a multiuser interference problem, we show that a very accurate estimate is obtained by finding the zeros of a decoupled set of 2nd and 3rd-order polynomials.

We then provide a novel, closed-form heuristic method of estimating the main-channel capacity with a modified asymptotic large-scale MIMO expression. This closed-form approximation is shown to perform well for cases of interest. Moreover, the complexity is unaffected by increases in number of antennas, which can quickly lead to dramatic increases computational complexity in Monte-Carlo simulations. Recent studies have used random matrix theory to characterize the *per receive antenna* capacity of MIMO systems by looking at the asymptotic large-antenna limit. Central to this theory is the idea that, in a MIMO system with t Tx antennas and r Rx antennas, the eigenvalues of many classes of random matrices converge almost surely to a non-random limit as $t, r \to \infty$ with the ratio $t/r \to \beta$ [85]. Large-scale analysis in such systems is often able to yield closed-form expressions, or greatly-reduced complexity solutions, for capacity in lieu of Monte-Carlo simulations. These solutions have been shown to be quite accurate even for realistically deployable finite numbers of antennas.

In [47], the asymptotic capacity of MIMO systems in the presence of multiple-antenna interferers is derived. While a closed-form solution is not possible in general (with the exception of the special case of equal number of antennas for all interfering and desired users), the capacity equation for a MIMO system with K interferers involves solving only a decoupled set of polynomials of order $K + 2$ and $K + 1$. We will demonstrate that the eavesdropper capacity required to determine the minimum guaranteed secrecy capacity in an AN system can be accurately represented within this multiple-antenna interferer framework. The approximation becomes tight for the assumed worst-case scenario of interest where Eve maximizes her SNR by physically moving herself very close to the Tx.

The large-antenna asymptotic capacity of a MIMO channel with full CSIT is derived in closed form in [86]. With AN secrecy assuming CSIT, these asymptotic techniques can be used to arrive at an approximation for the main channel capacity.

However, a key assumption in [86] is that SNR is sufficient such that all available spatial eigenmodes are utilized in the waterfilling power allocation. For the case of AN secrecy, a portion of the spatial dimensions available for signal transmission may be allocated instead to artificial noise transmission.

The asymptotic solutions we present in this chapter contribute to existing works in that they:

1. Extend previous asymptotic formulas to the MIMOME case and effectively incorporate the eigenmode partitioning central to AN secrecy methods;

2. Greatly reduce complexity (the eavesdropper channel is a solution of polynomial equations, while the main channel solution is closed-form) and demonstrate bounded error;

3. Apply to a more general channel model and thus depend only on parameters controllable at the transmitter; and

4. Yield more accurate results over SNRs of interest than previous approximation methods for the non-asymptotic cases (i.e. realizable number of antennas) tested.

3.2 System Model

We consider the standard MIMO wiretap channel, with t, r, and e antennas at transmitter Alice (Tx), receiver Bob (Rx) and eavesdropper Eve (Ex), respectively. $\mathbf{H} \in \mathbb{C}^{r \times t}$ is the MIMO main (Alice-Bob) channel matrix, and $\mathbf{G} \in \mathbb{C}^{e \times t}$ is the MIMO eavesdropper (Alice-Eve) channel matrix. We assume a rich scattering environment, and assume both channels to be slow flat-fading such that the channel is constant for the duration of the channel estimation and subsequent code word transmission. Thus the entries of $\mathbf{H}$ are i.i.d. complex Gaussian distributed. For comparison of antenna

configurations, we normalize the channel entries to have unit variance such that the average received SNR is independent of number of transmit antennas.

Following the MIMO AN procedure set forth in [21], Alice may attempt to give Bob a relative SNR advantage over Eve by broadcasting noise in the null space of Bob's channel. Alice and Bob first estimate the channel, and use singular value decomposition (SVD) to arrive at $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{\dagger}$, where † denotes the Hermitian transpose. Assuming $t > r$, there are a maximum of r dimensions on which Alice may transmit message symbols to Bob. However, Alice must have at least $e+1$ degrees of freedom available to devote to the AN symbols so that Eve is not able to overcome the added noise through linear combining. Alice chooses AN dimensions $d_a \geq e$, signal dimensions $d_s = \min(r, t-e)$, with $d_s + d_a \leq t$, and forms combined message symbol and noise symbol vector $\mathbf{w} = [\mathbf{w}_s^{\dagger}\mathbf{w}_a^{\dagger}]^{\dagger}$.

Alice chooses the precoding matrix to be a subset of vectors from the right singular vector matrix, split by columns according to number of signal and noise dimensions as $\mathbf{V} = [\mathbf{V}_s\ \mathbf{V}_a]$. The transmitted vector is thus $\mathbf{x} = [\mathbf{V}_s\ \mathbf{V}_a]\mathbf{w}$. The received vectors at Rx and Ex, respectively, become

$$\mathbf{U}_{d_s}^{\dagger}\mathbf{y}_m = \mathbf{U}_{d_s}^{\dagger}\mathbf{H}\mathbf{x} + \mathbf{U}_{d_s}^{\dagger}\mathbf{n}_m \tag{26}$$

$$= \mathbf{\Sigma}_{d_s}\mathbf{w}_s + \tilde{\mathbf{n}}_m \tag{27}$$

$$\mathbf{y}_e = \mathbf{G}\mathbf{x} + \mathbf{n}_e \tag{28}$$

$$= \mathbf{G}\mathbf{V}_s\mathbf{w}_s + \mathbf{G}\mathbf{V}_a\mathbf{w}_a + \mathbf{n}_e, \tag{29}$$

where the subscript d_s denotes the first d_s columns, and $\{\mathbf{n}_m, \mathbf{n}_e, \tilde{\mathbf{n}}_m\} \sim \mathcal{CN}(\{\mathbf{0}, \mathbf{0}, \mathbf{0}\}, \{\sigma_{n_m}^2\mathbf{I}_r, \sigma_{n_e}^2\mathbf{I}_e, \sigma_{\tilde{n}_m}^2\mathbf{I}_m\})$ are AWGN vectors at Rx and Ex, with the elements of $\tilde{\mathbf{n}}_m$ distributed identically to those of $\mathbf{n}_m$ since $\mathbf{U}$ is unitary. By Tx precoding with $\mathbf{V}$ and Rx processing with $\mathbf{U}$, Alice and Bob effectively turn the main channel into a bank of d_s parallel Gaussian channels, and, since the columns $\mathbf{V}$ are orthogonal, steer the noise into the null of the main channel. Eve, ignorant of $\mathbf{V}$ and $\mathbf{U}$, is unable

to avoid the effects of the added noise so long as her channel matrix entries are not strongly correlated with Bob's; this condition is commonly assumed to be true in a rich-scattering environment when Eve's distance from Bob exceeds a half-wavelength.

Alice may optimize secrecy by allocating power selectively to message and AN symbols. Defining message signal power $P_s = \mathrm{E}[\mathbf{w}_s^\dagger \mathbf{w}_s]$, and AN signal power $P_a = \mathrm{E}[\mathbf{w}_a^\dagger \mathbf{w}_a]$, the total transmit power is constrained to $P_s + P_a \leq P$. For a given P_s, Alice chooses the signal covariance matrix $\mathbf{R}_s = \mathrm{E}[\mathbf{w}_s \mathbf{w}_s^\dagger]$ through standard waterfilling [23]. Since $\mathbf{G}$ is unknown to Alice, the noise covariance matrix $\mathbf{R}_a = \mathrm{E}[\mathbf{w}_a \mathbf{w}_a^\dagger]$ is chosen as the scaled identity matrix.

The secrecy capacity of a three-party eavesdropper channel the non-negative maximum difference in mutual information between the main and eavesdropper channel [7],

$$C^{sec} = \max_{p(\mathbf{x})} [I(\mathbf{y}_m; \mathbf{x}) - I(\mathbf{y}_e; \mathbf{x})]^+, \tag{30}$$

where $p(\mathbf{x})$ is the input distribution of the message, $I(\mathbf{t}; \mathbf{u})$ is the mutual information between vectors $\mathbf{t}$ and $\mathbf{u}$, and $[x]^+ = \max(0, x)$. Assuming the channel transition probabilities are weakly symmetric, the secrecy capacity becomes the positive difference of main and eavesdropper channel capacities, $C^{sec} = (C^B - C^E)^+$. If the eavesdropper channel is noisier than the main channel, then $C^{sec} = C^B - C^E$. When AN is employed, the eavesdropper channel capacity can on average always be degraded to a value below that of the main channel capacity, guaranteeing a strictly positive ergodic secrecy capacity even when the Eve's received SNR is greater than Bob's. The AN-generated ergodic secrecy capacity is then

$$C^{sec} = \max_{\substack{(d_s, d_a) \in \mathcal{D} \\ (P_s, P_a) \in \mathcal{P}}} \mathrm{E}_{\mathbf{G},\mathbf{H}} [I(\mathbf{y}_m; \mathbf{x}) - I(\mathbf{y}_e; \mathbf{x})], \tag{31}$$

where

$$\mathcal{D} = \{(d_s, d_a) : \ d_a \geq e, \quad d_s \leq r, \quad d_s + d_a \leq t\} \tag{32}$$

$$\mathcal{P} = \{(P_s, P_a) : \ P_s + P_a \leq P\} \tag{33}$$

are the sets of dimension pairs and power-allocation pairs, respectively, that meet the AN problem requirements. Since the proximity of a passive Ex to the Tx is in general unknown, the ergodic minimum guaranteed secrecy capacity is often characterized by assuming the worst case eavesdropper noise scenario where $\sigma_{n_e}^2 \to 0$, given in [21] as:

$$\begin{aligned} C^{sec,mg} = \max_{\substack{(d_s,d_a)\in\mathcal{D} \\ (P_s,P_a)\in\mathcal{P}}} \mathrm{E}_{\mathbf{G},\mathbf{H}} \Bigg[& \log_2 \det\left(\mathbf{I}_r + \mathbf{H}\mathbf{R}_s\mathbf{H}^\dagger\right) \\ & - \log_2 \frac{\det\left(\mathbf{G}\mathbf{V}_s\mathbf{R}_s\mathbf{V}_s^\dagger\mathbf{G}^\dagger + \mathbf{G}\mathbf{V}_a\mathbf{R}_a\mathbf{V}_a^\dagger\mathbf{G}^\dagger\right)}{\det(\mathbf{G}\mathbf{V}_a\mathbf{R}_a\mathbf{V}_a^\dagger\mathbf{G}^\dagger)} \Bigg], \end{aligned} \tag{34}$$

where $\sigma_{n_m}^2 = 1$ and a mutual-information-maximizing Gaussian signaling alphabet have been assumed.

We note that, in contrast to [45], our work is similar to [21] in that we require all AN to be transmitted in the null-space of the main channel, and the equations we derive may thus be suboptimal with regards to the rates they generate. However, the advantage gained by this relaxation diminishes quickly with increases in Tx antennas; the effect is most noticed with two transmit antennas, and with only four antennas at Tx the secrecy capacity is nearly identical to the zero-forcing approach. Besides diminishing returns, there are numerous other reasons to limit AN to the null-space of the main channel, the most salient of which is to avoid solving another optimization problem for each iteration of the capacity calculation. Thus, while optimal transmit covariance matrix for the MIMOME case remains an open problem, from here forward we assume that the number of antennas at Tx to be four at a minimum, and we use the term "secrecy capacity" assuming AN is transmitted only in the null space of the main channel.

3.3 Large-Scale MIMO Analysis

Since the secrecy capacity (31) is in general non-convex, both rates must be calculated once for each point in $\mathcal{D}$ and $\mathcal{P}$. The number of acceptable dimension pairs $|\mathcal{D}|$ is predetermined by the MIMO antenna configuration, while the number of acceptable power-allocation pairs $|\mathcal{P}|$ will depend on the resolution chosen. After these $2(|\mathcal{D}| \times |\mathcal{P}|)$ rates are calculated, the maximum can be found via exhaustive search. It is easily seen that the size of the search space can quickly grow large as number of antennas increase or desired resolution decreases. Therefore an efficient method of calculating the Rx and Ex rates is of great interest in any system, particularly those that may be resource-constrained or adaptive in time.

We now present the main results of this chapter by deriving accurate, low-complexity approximations to the minimum-guaranteed secrecy capacity for the MIMOME case. We proceed by analyzing the Ex and Rx terms in (34) independently. This produces values for the respective communication rates achieved by Bob and Eve,

$$R^B = I(\mathbf{y}_m, \mathbf{x}), \quad \text{and} \quad R^E = I(\mathbf{y}_e, \mathbf{x}). \tag{35}$$

The procedure for calculation of these rates is as follows. First, we reformulate the eavesdropper channel into a multiuser interference framework to allow for partitioning of eigenmodes, and approximate using large-scale asymptotic analysis results from random matrix theory. We show also that a reduction in search space is possible with this new approach. Next, we provide a heuristic approach to modify existing main-channel capacity methods which is simple, intuitive, and accounts for the necessary eigenmode partitioning. With closed-form solutions for both Ex and Rx channels, the secrecy capacity is then easily and quickly approximated.

We note that a large-scale analysis is included in [21] which defines the minimum guaranteed secrecy capacity in terms of the expectation of eigenvalues of the eavesdropper channel. This expectation is evaluated via numerical integration of a

partitioned and weighted probability density function (PDF) of the eigenvalues of a Wishart channel-covariance matrix. However, the large-scale MIMO approximation we present here circumvents the expectation process altogether, allowing for a closed-form expression and even further reduction in computational complexity.

We now provide an approximation to the first term in (31). Whereas non-asymptotic capacities require specific number of antennas at Tx, Rx and Ex, we require only that the ratios of antennas is held constant and allow the number of antennas to grow without bound. Since the AN symbols transmitted can be chosen to be independent of all message symbols, we can view the AN as though it were actually message symbols coming from an outside interfering user. Thus, the Ex will observe d_s message symbols from the Tx, corrupted by additive white Gaussian noise (AWGN) and d_a message symbols from a theoretical unknown user. We will use this multiuser-interference approach to approximate the per-eavesdrop antenna capacity

$$\mathcal{R}^{\mathrm{E}} = \frac{1}{e} R^{\mathrm{E}}. \tag{36}$$

3.3.1 Existing Asymptotic Capacity Results

In approximating the secrecy capacity generated by AN, we will make use of the following Lemmas:

Lemma 1. [74] *For an $m \times n$ MIMO wireless communication channel $\mathbf{G}$ with i.i.d. entries of arbitrary distribution and unit variance, signal to noise ratio SNR, and diagonal matrix $\mathbf{Q}$,*

$$C = \mathrm{E}\left[\log_2 \det\left(\mathbf{I}_n + \frac{\mathrm{SNR}}{m}\mathbf{G}\mathbf{Q}\mathbf{G}^{\dagger}\right)\right], \tag{37}$$

where expectation is over the random channel gains $\mathbf{G}$, can be written in per-receive-antenna asymptotic form as $m, n \to \infty$ with $m/n \to \beta$:

$$\frac{1}{n}C = \beta E\left[\log_2\left(1 + \frac{\mathrm{SNR}}{\beta}\eta\lambda(\mathbf{Q})\right)\right] + \log_2\left(\frac{1}{\eta}\right) + \eta\log_2(e), \tag{38}$$

where expectation is over the eigenvalues of $\mathbf{Q}$*, denoted* $\lambda(\mathbf{Q})$*, and* $\eta \in [0,1]$ *satisfies the Tse-Hanly* [84] *equation*

$$\eta + \beta E\left[\frac{\mathrm{SNR}\lambda(\mathbf{Q})\eta}{\mathrm{SNR}\lambda(\mathbf{Q})\eta + \beta}\right] = 1. \tag{39}$$

Lemma 2. [47] *In a* $m \times n$ *MIMO communication channel* $\mathbf{G}_0$ *with signal to additive white Gaussian noise (AWGN) ratio* SNR *in the presence of interference from* $k = 1 \ldots K$ *outside interferers, each with signal-to-interference ratio* SIR_k *and* m_k *antennas producing MIMO interference channel* $\mathbf{G}_k$*. Then the AWGN+K interferer-limited capacity is*

$$C^{AWGN+K} = \mathrm{E}\Bigg[\log_2\det\Big(\mathbf{I}_n + \frac{\mathrm{SNR}}{m}\mathbf{G}_0\mathbf{G}_0^\dagger + \sum_{k=1}^{K}\frac{\mathrm{SNR}}{m_k\mathrm{SIR}_k}\mathbf{G}_k\mathbf{G}_k^\dagger\Big) - \log_2\det\Big(\mathbf{I}_n + \sum_{k=1}^{K}\frac{\mathrm{SNR}}{m_k\mathrm{SIR}_k}\mathbf{G}_k\mathbf{G}_k^\dagger\Big)\Bigg], \tag{40}$$

with expectation over the random channel gains. After defining the block matrices:

$$\mathcal{G}_2 = [\mathbf{G}_1\ \mathbf{G}_2\ \ldots\ \mathbf{G}_K], \tag{41}$$

$$\mathcal{G}_1 = [\mathbf{G}_0\ \mathcal{G}_2], \tag{42}$$

$$\mathbf{B}_2 = \begin{bmatrix} \frac{m}{m_1\mathrm{SIR}_1}\mathbf{\Theta}_1 & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \frac{m}{m_2\mathrm{SIR}_2}\mathbf{\Theta}_2 & \ldots & \mathbf{0} \\ \vdots & \vdots & \ddots & \mathbf{0} \\ \mathbf{0} & \ldots & \mathbf{0} & \frac{m}{m_K\mathrm{SIR}_K}\mathbf{\Theta}_K \end{bmatrix}, \tag{43}$$

$$\mathbf{B}_1 = \begin{bmatrix} \mathbf{\Theta} & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_2 \end{bmatrix}, \tag{44}$$

equation (40) can be written as the difference $C^{\mathrm{AWGN+K}} = C_1 - C_2$*, with*

$$C_1 = \mathrm{E}\left[\log_2\det\left(\frac{\mathrm{SNR}}{m}\mathcal{G}_1\mathbf{B}_1\mathcal{G}_1^\dagger\right)\right] \tag{45}$$

$$C_2 = \mathrm{E}\left[\log_2\det\left(\frac{\mathrm{SNR}}{m}\mathcal{G}_2\mathbf{B}_2\mathcal{G}_2^\dagger\right)\right]. \tag{46}$$

Let $m, n \to \infty, \beta \to m/n$, and let $m_k \to \infty, \beta_k = m_k/n$ for $k = 1 \dots K$. Then, using Lemma 1, the per-receive antenna capacity can be determined through

$$\frac{1}{n} C^{AWGN+K} \doteq \mathcal{C}^{AWGN+K} = \mathcal{C}_1 - \mathcal{C}_2, \tag{47}$$

where

$$\mathcal{C}_1 = \left(\beta + \sum_{k=1}^{K} \beta_k\right) \mathrm{E}\left[\log_2\left(1 + \mathrm{SNR}\frac{\eta_1}{\beta} B_1\right)\right] + \log_2 \frac{1}{\eta_1} + (\eta_1 - 1)\log_2(e), \tag{48}$$

$$\mathcal{C}_2 = \left(\sum_{k=1}^{K} \beta_k\right) \mathrm{E}\left[\log_2\left(1 + \mathrm{SNR}\frac{\eta_2}{\beta} B_2\right)\right] + \log_2 \frac{1}{\eta_2} + (\eta_2 - 1)\log_2(e), \tag{49}$$

η_1, η_2 are the respective solutions to

$$\eta_1 + \left(\beta + \sum_{k=1}^{K} \beta_k\right) \mathrm{E}\left[\frac{\mathrm{SNR}\eta_1 B_1}{\mathrm{SNR}\eta_1 B_1 + \beta}\right] = 1, \tag{50}$$

$$\eta_2 + \left(\sum_{k=1}^{K} \beta_k\right) \mathrm{E}\left[\frac{\mathrm{SNR}\eta_2 B_2}{\mathrm{SNR}\eta_2 B_2 + \beta}\right] = 1, \tag{51}$$

expectations are taken with respect to B_1 and B_2, random variables distributed as the respective asymptotic empirical eigenvalue distributions of matrices $\mathbf{B}_1$ and $\mathbf{B}_2$, $\mathbf{\Theta}$ is the transmit covariance matrix of the desired user, $\mathbf{\Theta}_k$ is the transmit covariance matrix of the kth interferer, and $\mathbf{0}$ denotes an all-zero matrix.

Lemma 3. [86] *Assume an $r \times t$ MIMO channel with $t > r$, i.i.d. channel entries, transmit power P, and full channel state information at the transmitter. Let $t, r \to \infty$, and $t/r \to \beta$. Then, for P sufficient to waterfill over all r eigenmodes, a closed-form solution for the asymptotic per-antenna channel capacity is given as*

$$\mathcal{C}(P, \beta) = \log_2\left(\beta P + \frac{\beta}{\beta - 1}\right) + (\beta - 1)\log_2\left(\frac{\beta}{\beta - 1}\right) - \log_2 \mathrm{e}. \tag{52}$$

3.3.2 Large-Scale MIMO Eavesdropper Capacity Approximation

Lemmas 1 and 2 will form the foundation for our eavesdropper channel approximation. However, these Lemmas cannot directly be applied as is since they make no allowance

Table 1: Variables and definitions.

Variable (**units**)	**Definition**
d_s (dimensions)	eigenmodes devoted to signal transmission
d_a (dimensions)	eigenmodes devoted to AN transmission
α (unitless)	proportion of total power devoted to signal
β (unitless)	Tx antenna to Rx antenna ratio
γ_s (dim/ant)	signal eigenmodes to total eigenmodes ratio
γ_a (dim/ant)	AN eigenmodes to total eigenmodes ratio
ζ_s (dim/ant)	signal eigenmodes to Rx antenna ratio

for varying the number of eigenmodes allocated to either signal or AN; rather, they simply assume that all eigenmodes available to transmitter and all outside interferers are utilized. To see this, notice that the equations for $\mathcal{C}_1, \mathcal{C}_2, \eta_1$, and η_2 are not functions of eigenmodes, but rather simply of antenna ratios. If we were to implement these lemmas directly, we could vary eigenmode allocation over all possible pairs $(d_s, d_a) \in \mathcal{D}$ without changing the resulting output.

We will maintain the β notation, as in Lemmas 1 and 2, to denote the asymptotic ratio of Tx to Rx (or Tx to Ex, for the eavesdropper channel) antennas. To allow variations in eigenmode allocations, we introduce two new quantities,

$$\gamma_s = \lim_{d_s, t \to \infty} \frac{d_s}{t}, \quad \text{and} \quad \gamma_a = \lim_{d_a, t \to \infty} \frac{d_a}{t}, \tag{53}$$

which represent the asymptotic fraction of total eigenmodes devoted to signal and AN, respectively. For easy reference, the variables defined in the following analyses are summarized in Table 1.

Proposition 1. *In a MIMO wireless channel with t transmit and e eavesdrop antennas, assume the transmitter chooses to transmit d_s information symbols and $d_a \geq e$ AN symbols. Define the ratio of signal power to total power as $\alpha = \frac{P_s}{P_s + P_a}$. Let $t, e \to \infty$, with $t/e \to \beta$, $d_s/t \to \gamma_s$, and $d_a/t \to \gamma_a$. Then the worst-case (eavesdropper SNR $\to \infty$) per-antenna eavesdropper rate can be approximated in closed-form*[2]

[2] *Writing the closed-form solution to the eavesdropper-channel efficiencies η_1 and η_2 is possible*

as:

$$\mathcal{R}^E \approx (\gamma_s+\gamma_a)\,\beta\left[\gamma_s \log_2\left(1+\alpha P\frac{\eta_1}{\gamma_s^2\beta}\right)+\gamma_a\log_2\left(1+(1-\alpha)P\frac{\eta_1}{\gamma_s\gamma_a\beta}\right)\right]$$
$$-\gamma_a\beta\left[\log_2\left(1+(1-\alpha)P\frac{\eta_2}{\gamma_s\gamma_a\beta}\right)\right]+\log_2\left(\frac{\eta_2}{\eta_1}\right)+(\eta_1-\eta_2)\log_2(e), \quad (54)$$

where η_1 and η_2 are the solutions on interval $[0,1]$ to the following:

$$\eta_1+(\gamma_s+\gamma_a)\,\beta\left[\frac{\gamma_s\alpha P\eta_1}{\alpha P\eta_1+\gamma_s^2\beta}+\frac{\gamma_a(1-\alpha)P\eta_1}{(1-\alpha)P\eta_1+\gamma_s\gamma_a\beta}\right]=1 \quad (55)$$

$$\eta_2+\gamma_a\beta\left[\frac{(1-\alpha)P\eta_2}{(1-\alpha)P\eta_2+\gamma_s\gamma_a\beta}\right]=1 \quad (56)$$

Proof. We begin with the expression for eavesdropper rate R^E in (35). For a given set of signal and AN covariance matrices (i.e. for a fixed power allocation and antenna allocation),

$$R^E=\mathrm{E}_{\mathbf{G}}\left[\log_2\frac{\det\left(\mathbf{G}\mathbf{V}_s\mathbf{R}_s\mathbf{V}_s^\dagger\mathbf{G}^\dagger+\mathbf{G}\mathbf{V}_a\mathbf{R}_a\mathbf{V}_a^\dagger\mathbf{G}^\dagger\right)}{\det(\mathbf{G}\mathbf{V}_a\mathbf{R}_a\mathbf{V}_a^\dagger\mathbf{G}^\dagger)}\right]. \quad (57)$$

Finding the eavesdropper rate involves taking the expectation over the random channel gains between Tx and Ex. However, using results from random matrix theory and Lemma 1, this quantity can instead be computed for high SNR through expectation over eigenmode power allocation, which is controllable at the Tx.

To recast the eavesdropper rate from the AN setup into a multiuser interference framework, we make two key assumptions:

1. The message symbols are sent by the Tx through use of d_s antennas, while the AN symbols can be thought of as coming from a separate, unknown outside transmitter with d_a antennas.

2. The power allocated to message symbols is uniformly distributed over the d_s eigenmodes.

using the quadratic and cubic (Cardano) equations. However, doing so gives lengthy and cumbersome results that do not yield additional insight. Therefore in this chapter we refer to the eavesdropper results as closed form while leaving them as solutions to 2nd and 3rd-order polynomials.

Alice first designs the signal and AN covariance matrices $\mathbf{R}_s$ and $\mathbf{R}_a$, which are then spread over the entirety of her t antennas with the right singular vectors of the main channel to form the transmit correlation matrices $\mathbf{V}_s\mathbf{R}_s\mathbf{V}_s^\dagger$ and $\mathbf{V}_a\mathbf{R}_a\mathbf{V}_a^\dagger$. We can instead apply the singular vectors to the channel matrix $\mathbf{G}$ such that $\mathbf{G}_s = \mathbf{G}\mathbf{V}_s$ and $\mathbf{G}_a = \mathbf{G}\mathbf{V}_a$. Note that, because $\mathbf{V}_s$ and $\mathbf{V}_a$ are unitary matrices, $\mathbf{G} \equiv [\mathbf{G}_s\mathbf{G}_a]$ in distribution, and we can then write

$$R^E = \mathrm{E}_{\mathbf{G}_s,\mathbf{G}_a}\left[\log_2 \frac{\det\left(\mathbf{G}_s\mathbf{R}_s\mathbf{G}_s^\dagger + \mathbf{G}_a\mathbf{R}_a\mathbf{G}_a^\dagger\right)}{\det(\mathbf{G}_a\mathbf{R}_a\mathbf{G}_a^\dagger)}\right]. \tag{58}$$

To maximize the rate over the main channel, Alice would use the standard waterfilling procedure over d_s eigenmodes to design $\mathbf{R}_s$. However, for the eavesdropper channel we assume the worst-case scenario where Eve is able to boost her SNR by moving closer to the Tx. It is well known that as SNR grows large, the waterfilling solution converges to the uniform distribution. Thus, our second assumption above is valid for approximating R^E as SNR grows large. The assumption of a uniform distribution also enables finding a closed-form solution, since the polynomial order of (55) and (56) increases by one for each additional unique power level allocated.

With $\alpha = \frac{P_s}{P}$ as the proportion of power allocated to signal transmission, the proportion of AN power is then $(1-\alpha) = \frac{P_a}{P}$. For convenience we assume the receiver noise to have unit variance, thus SNR $= P$. Our eavesdropper rate then becomes:

$$R^E = \mathrm{E}_{\mathbf{G}_s,\mathbf{G}_a}\left[\log_2 \frac{\det\left(\frac{\alpha P}{d_s}\mathbf{G}_s\mathbf{G}_s^\dagger + \frac{(1-\alpha)P}{d_a}\mathbf{G}_a\mathbf{G}_a^\dagger\right)}{\det\left(\frac{(1-\alpha)P}{d_a}\mathbf{G}_a\mathbf{G}_a^\dagger\right)}\right] \tag{59}$$

$$= \mathrm{E}_{\mathbf{G}_s,\mathbf{G}_a}\left[\log_2\det\left(\frac{P}{t}[\mathbf{G}_s\mathbf{G}_a]\begin{bmatrix}\frac{\alpha t}{d_s}\mathbf{I}_{d_s} & \mathbf{0}\\ \mathbf{0} & \frac{(1-\alpha)t}{d_a}\mathbf{I}_{d_a}\end{bmatrix}\begin{bmatrix}\mathbf{G}_s^\dagger\\ \mathbf{G}_a^\dagger\end{bmatrix}\right)\right] \tag{60}$$

$$- \mathrm{E}_{\mathbf{G}_a}\left[\log_2\det\left(\frac{P}{t}\mathbf{G}_a\begin{bmatrix}\frac{(1-\alpha)t}{d_a}\mathbf{I}_{d_a}\end{bmatrix}\mathbf{G}_a^\dagger\right)\right]. \tag{61}$$

Defining

$$\mathbf{\Phi_1} = \begin{bmatrix} \frac{\alpha}{\gamma_s}\mathbf{I}_{d_s} & \\ & \frac{1-\alpha}{\gamma_a}\mathbf{I}_{d_a} \end{bmatrix}, \tag{62}$$

$$\mathbf{\Phi_2} = \frac{1-\alpha}{\gamma_a}\mathbf{I}_{d_a}. \tag{63}$$

the eavesdropper rate becomes

$$R^E = \mathrm{E}\left[\log_2\det\left(\frac{P}{t}\mathbf{G}\mathbf{\Phi}_1\mathbf{G}^\dagger\right)\right] - \mathrm{E}\left[\log_2\det\left(\frac{P}{t}\mathbf{G}_a\mathbf{\Phi}_2\mathbf{G}_a^\dagger\right)\right], \tag{64}$$

which is now in the form of $R_1 - R_2$ similar to (45) and (46) for high SNR. Each term can subsequently be solved using Lemma 2, instead of taking expectation over random channel gains, but rather by expectation over eigenvalues of matrices $\mathbf{\Phi}_1$ and $\mathbf{\Phi}_2$. Because $\mathbf{\Phi}_1$ and $\mathbf{\Phi}_2$ are diagonal, their eigenvalue distributions are simply:

$$\lambda(\mathbf{\Phi}_1) = \begin{cases} \frac{\alpha}{\gamma_s}, & \text{with probability } \gamma_s \\ \frac{1-\alpha}{\gamma_a}, & \text{with probability } \gamma_a \end{cases} \tag{65}$$

$$\lambda(\mathbf{\Phi}_2) = \frac{1-\alpha}{\gamma_a}, \quad \text{with probability } 1. \tag{66}$$

This transformation is notable, since, as demonstrated in [21], previous attempts at calculating the ergodic capacity over a subset of eigenmodes require integration of a continuous eigenvalue distribution (as detailed in the following Partial PDF Integration subsection), as well as numerical calculation of the lower limit. In contrast, these new eigenvalue distributions are in fact probability mass functions, and each expectation in (64) can now be directly evaluated with a summation. The eigenmodes can then be partitioned to signal and AN, respectively, as $\gamma_a\beta$ and $\gamma_s\beta$, and combining (48), (50) and taking expectation over (65), the first term in (64) yields

$$R_1 = (\gamma_s + \gamma_a)\beta\left[\log_2\left(1 + P\frac{\eta_1}{\gamma_s\beta}\left(\frac{\alpha}{\gamma_s}\right)\right)(\gamma_s) + \log_2\left(1 + P\frac{\eta_1}{\gamma_s\beta}\left(\frac{1-\alpha}{\gamma_a}\right)\right)(\gamma_a)\right], \tag{67}$$

with η_1 solving

$$\eta_1 + (\gamma_s + \gamma_a)\,\beta \left[\frac{P\eta_1(\frac{\alpha}{\gamma_s})}{P\eta_1(\frac{\alpha}{\gamma_s}) + \gamma_s\beta}\,(\gamma_s) + \frac{P\eta_1(\frac{1-\alpha}{\gamma_a})}{P\eta_1(\frac{1-\alpha}{\gamma_a}) + \gamma_s\beta}\,(\gamma_a) \right] = 1. \tag{68}$$

Similarly, combining (49), (51), and (66), the second term in (64) yields

$$R_2 = \gamma_a\beta \left[\log_2 \left(1 + P\frac{\eta_2}{\gamma_s\beta} \left(\frac{1-\alpha}{\gamma_a} \right) \right) \right], \tag{69}$$

with η_2 solving

$$\eta_2 + \gamma_s\beta \left[\frac{P\eta_2(\frac{1-\alpha}{\gamma_a})}{P\eta_2(\frac{1-\alpha}{\gamma_a}) + \gamma_s\beta} \right] = 1. \tag{70}$$

To find the per-antenna rates we set $\mathcal{R}_1 = \frac{1}{e}R_1$ and $\mathcal{R}_2 = \frac{1}{e}R_2$. Finally, subtracting $\mathcal{R}_1 - \mathcal{R}_2$, we arrive at the proof. □

Although we assume an i.i.d. Gaussian channel model here for comparison with previous literature, the derivation in Appendix 3.3.2 only requires i.i.d. channel entries. Note that the expectation over complex channel gains $\mathbf{H}$ and $\mathbf{G}$ has been replaced in the asymptotic analysis with the solution to a pair of polynomials in η_1 and η_2. These polynomials are also decoupled, which further reduces the complexity required to solve the system.

Thus for a given pair $(d_s, d_a) \in \mathcal{D}$, the worst-case reduction in secrecy capacity arising from an eavesdropper of unknown location can be estimated simply by solving for η_1 and η_2 and plugging the values into (54). This amounts to finding the zeros of a set of decoupled quadratic and cubic equations. Note that the secrecy capacity equation given in (34) is, in general, non-convex, and efficient optimization methods remain an open problem. The reduction in complexity afforded by the multiuser interference approximation method will be further scaled by the number of search points employed by the specific optimization method chosen, for which we introduce the following proposition.

Proposition 2. *The set of eigenmode allocation pairs $(d_s, d_a) \in \mathcal{D}$ over which to maximize secrecy rates can be reduced to a subset $\mathcal{D}' \subseteq \mathcal{D}$ by adding the constraint that*

$$d_a \geq \lceil \sqrt{et} - d_s \rceil, \tag{71}$$

where $\lceil x \rceil$ is the smallest integer greater than or equal to x.

Proof. The values η_1 and η_2 can be interpreted as multiuser efficiencies [88] , and, to maximize the secrecy rate, the efficiencies for the Ex channel should equal zero. The minimum-guaranteed secrecy occurs when $P \to \infty$. Rewriting (50) as

$$\eta_1 + \frac{d_s + d_a}{e} \left[\frac{1}{\frac{t}{d_s} + \frac{d_s}{e\alpha P \eta_1}} + \frac{1}{\frac{t}{d_a} + \frac{d_s}{e(1-\alpha) P \eta_1}} \right] = 1, \tag{72}$$

the asymptotic power limit becomes

$$\lim_{P \to \infty} \eta_1 = \left[1 - \frac{(d_s + d_a)^2}{et} \right]^+, \tag{73}$$

which is zero for all

$$\frac{(d_s + d_a)^2}{et} \geq 1. \tag{74}$$

Since eigenmodes are constrained to be integer-valued, we arrive at $d_a \geq \lceil \sqrt{et} - d_s \rceil$. □

If Alice is, perhaps sub-optimally, constricted to exhaust all available eigenmodes on either signal or AN such that $d_s + d_a = t$, then $\eta_1 = 0$ for $t \geq e$. Without $t \geq e$ the AN approach to secrecy is not possible, so in this restrictive case no new information is gained. However, in such a case the search space would already be greatly reduced. Note that we can similarly look at the asymptotic power limit of η_2 by rewriting (51) as

$$\eta_2 + \frac{1}{\frac{e}{d_a} + \frac{d_s}{(1-\alpha) t P \eta_2}} = 1, \tag{75}$$

the asymptotic limit becomes

$$\lim_{P\to\infty} \eta_2 = \left[1 - \frac{d_a}{e}\right]^+, \tag{76}$$

which yields the requirement that $d_a \geq e$. This requirement was presented originally in [21] as a condition to ensure a nonzero determinant in the denominator of the minimum guaranteed secrecy capacity equation (34). The analysis here confirms the earlier result from a multiuser interference approach.

Figure 7 shows an example of how eigenmode allocation and power affect Ex efficiencies η_1 and η_2. As expected, both efficiencies are shown to decay more quickly with each additional eigenmode allocated to AN. For the case of $\beta = 3$ shown, both η_1 and η_2 approach zero for sufficient transmit power, thereby limiting the advantage any eavesdropper is able to gain by moving physically closer to the Tx. Figure 8 shows that the reduced search space achieved by imposing the additional eigenmode restriction from Proposition 2 has eliminated the eigenmode pairs smallest in numbers. It is quite intuitive that Alice would not benefit from using only a small fraction of available eigenmodes; this fact is now confirmed from the multiuser-interference perspective.

3.3.3 Main Channel: Partial-PDF Integration (PPI)

Closed-form solutions for the ergodic capacity in a strictly AWGN-limited channel has been studied extensively, and appears in various forms in [85, 67, 86]. However, all previous closed-form solutions require all available eigenmodes are allocated signal power. Therefore, a new strategy must be devised when only some eigenmodes are used. In [21], the eigenvalue PDF is integrated from a lower limit found numerically instead of the minimum eigenvalue.

To review this process, assume an $r \times t$ zero-mean i.i.d. channel $\mathbf{H}$, with $r, t \to \infty$ and $r/t \to \rho = 1/\beta$, the PDF of the eigenvalues of the Wishart channel covariance

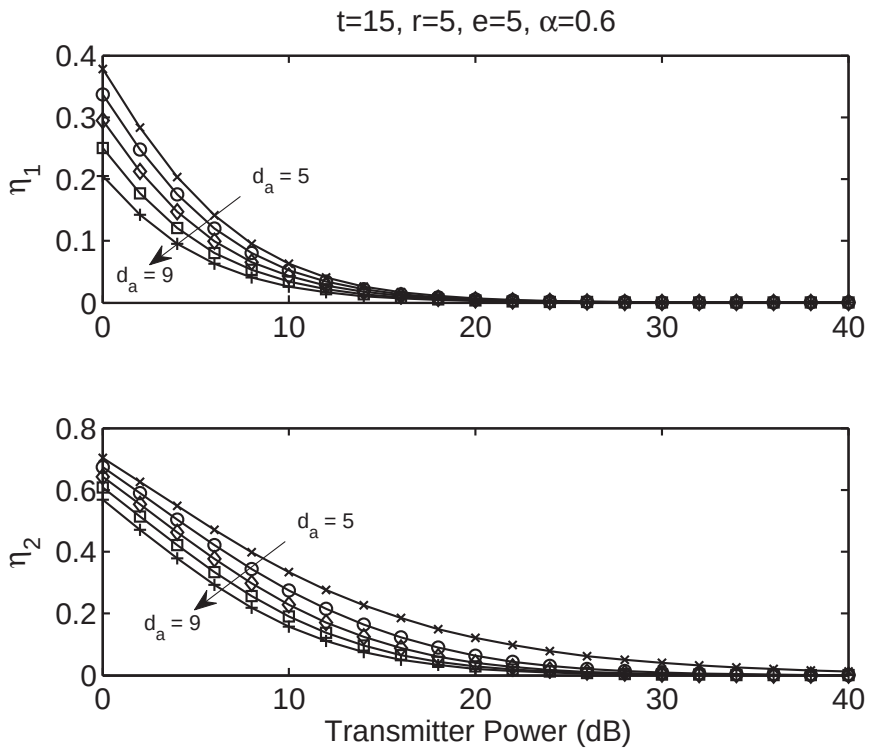


Figure 7: Example eavesdropper efficiencies η_1 and η_2 as a function of transmit power P.

matrix $\mathbf{HH}^\dagger$ converges almost surely [85] as

$$f(\lambda) = \delta(\lambda)(1-\rho)^+ + \frac{\sqrt{(\lambda - a(\rho))^+ (b(\rho) - \lambda)^+}}{2\pi\lambda}, \tag{77}$$

with minimum and maximum eigenvalues $a(\rho) = \left(1 - \sqrt{\rho}\right)^2$, and $b(\rho) = \left(1 + \sqrt{\rho}\right)^2$, respectively, and where $\delta(x)$ is the Dirac-delta function. For AN systems, $\rho < 1$, and $(1-\rho)$ of the probability occurs at $\lambda = 0$. However, we are concerned only with the non-zero eigenvalues for message transmission, and thus we can isolate and normalize the PDF as

$$f(\lambda > 0) = \frac{\sqrt{(\lambda - a(\rho))^+ (b(\rho) - \lambda)^+}}{2\pi\rho\lambda}. \tag{78}$$

In the large-antenna asymptotic limit, the per-user capacity is

$$\bar{C} = \sum_{i=1}^{r} \log\left(1 + \frac{\lambda_i}{\sigma_n^2}\right), \tag{79}$$

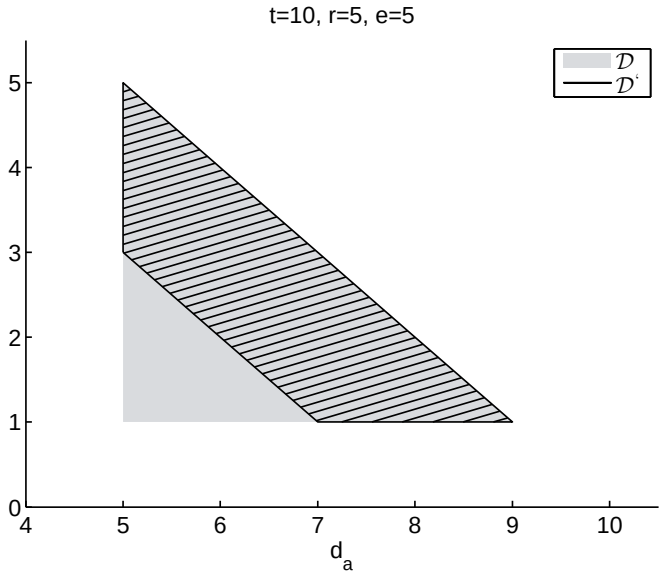


Figure 8: Example reduction in search space from $\mathcal{D}$ (gray) to $\mathcal{D}$ (lines) as a result of adding the restriction in Proposition 2.

where σ_n^2 is the receiver noise, converges almost surely [67] to the integral representation

$$\bar{C} = \int_0^\infty \log\left(1 + \frac{\lambda}{\sigma_n^2}\right) \frac{\sqrt{\left(\lambda - a\left(\rho\right)\right)^+ \left(b\left(\rho\right) - \lambda\right)^+}}{2\pi\rho\lambda} d\lambda. \tag{80}$$

Substituting the power allocation for the main channel, and scaling by ρ to fulfill the signal power constraint, and defining the per-receive antenna capacity as

$$\mathcal{C}^B = \frac{1}{r} C^B \tag{81}$$

the main channel capacity becomes

$$\mathcal{C}^B = \int_0^\infty \log\left(1 + \frac{\alpha P \lambda}{\rho}\right) \frac{\sqrt{\left(\lambda - a\left(\rho\right)\right)^+ \left(b\left(\rho\right) - \lambda\right)^+}}{2\pi\rho\lambda} d\lambda. \tag{82}$$

Since $r \to \infty$, the d_s largest eigenvalues can be selected by changing the lower limit of the integral to a value λ^* which, integrated over the PDF alone yields a value of d_s/r. In [21], the same result is achieved by scaling the PDF by constant ν such that $\int_{\lambda^*}^\infty \nu f(\lambda) d\lambda = 1$. Although we have explicit formulas for the minimum and maximum

eigenvalue, no such expressions for a general partitioning to d_s/r exist and the values of λ^* must be calculated numerically.

Nonetheless, we compare this approach in both to the new large-scale approximation we present in closed form in the following section. We find that, though both asymptotic techniques yield similar results for the small-scale MIMO systems we study, the large-scale closed-form solution approximation outperforms the numerical PPI approach in both accuracy and complexity for the cases tested.

3.3.4 Main Channel: Large-Scale Approximation (LSA)

Once again we see that this solution is not directly applicable to the AN problem since it is a function of the antenna ratio only, and not of eigenmodes. We will retain the β and γ_s notation from Proposition 1, and define the new quantity

$$\lim_{r,d_s\to\infty} \frac{r}{d_s} = \zeta_s \tag{83}$$

as the asymptotic ratio of Rx antennas to signal eigenmodes.

Proposition 3. *In a MIMO system with t transmit and r receive antennas, with $t > r$, define the number of eigenmodes allocated to signal transmission $d_s \leq r$. Let $t, r \to \infty$, $t/r \to \beta$, $d_s/t \to \gamma_s$, and $r/d_s \to \zeta_s$. Define $\alpha = P_s/P$ as the ratio of signal to total power transmitted. Then the per-antenna main-channel rate can be approximated by:*

$$\mathcal{R}^B \approx \frac{1}{\zeta_s}\left[\log_2\left(\frac{\alpha P}{\gamma_s} + \frac{1}{1-\gamma_s}\right) + \frac{1-\gamma_s}{\gamma_s}\log_2\left(\frac{1}{1-\gamma_s}\right) - \log_2 \mathrm{e}\right]. \tag{84}$$

Proof. The closed form capacity given in Lemma 3 is a function only of β and SNR. As seen in the preceding discussion of PPI, it is not possible to write one expression for any arbitrary ordered eigenvalue of a Wishart matrix; rather it must be calculated numerically. To make the problem of a closed-form solution accounting for a variable number of eigenmodes tractable, we make the simplifying assumption that the receiver

will only use as many reception antennas as are set as d_s at the Tx. The effect is that the antenna ratio β in (52) becomes $\zeta_s\beta$, and the rate becomes

$$\frac{1}{d_s}R^B = \log_2\left(\zeta_s\beta\alpha P + \frac{\zeta_s\beta}{\zeta_s\beta - 1}\right) + (\zeta_s\beta - 1)\log_2\left(\frac{\zeta_s\beta}{\zeta_s\beta - 1}\right) - \log_2 \mathrm{e}. \tag{85}$$

$$= \log_2\left(\frac{\alpha P}{\gamma_s} + \frac{1}{1-\gamma_s}\right) + \frac{1-\gamma_s}{\gamma_s}\log_2\left(\frac{1}{1-\gamma_s}\right) - \log_2 \mathrm{e}. \tag{86}$$

Finally, noting that MIMO capacities are well known to grow linearly with $\min(t, r)$ at high SNR, we can properly scale the $1/d_s$ rate to the desired $1/r$ rate by multiplying by $1/\zeta_s$ to arrive at $\mathcal{R}^B$. □

The approximation of the main channel capacity is given in closed form. Intuitively, this approximation can be thought of as a scaling of the asymptotic antenna ratio β by r/d_s to reflect the reduction in signal dimensions, and subsequent scaling of the asymptotic capacity by d_s/r to transform the units of the result from bps/Hz per signal dimension to bps/Hz per receive antenna. Though this analysis is heuristic, we will see that the performance is nonetheless good for the cases tested.

Proposition 4. *Define the approximation error incurred by using the large-scale asymptotic approximation in (84) as*

$$\epsilon = \frac{1}{r}\mathrm{E}_{\mathbf{H}}\left[\log_2 \det\left(\mathbf{I}_r + \mathbf{H}\mathbf{V}_s\mathbf{R}_s\mathbf{V}_s^\dagger\mathbf{H}^\dagger\right)\right] - \mathcal{R}^B. \tag{87}$$

The magnitude of this approximation error is upper-bounded by

$$|\epsilon| \leq \frac{\log_2(\mathrm{e})}{\zeta_s}. \tag{88}$$

Proof. Since the asymptotic formulas presented rely on antenna ratios rather than absolute numbers, and since both $t/r > 1$ and $t/d_s > 1$, the transformation in (84) of antenna ratio from t/r to t/d_s is equivalent to forming the product $\frac{(r/d_s)t}{r}$. This can be interpreted as holding r constant while increasing t (since $r/d_s \geq 1$). In a MIMO system limited purely by AWGN, the per-receive antenna effect of adding extra antennas

at the Tx was shown in [47] to be strictly limited as $\mathcal{C}(\text{SNR}, \beta = \infty) - \mathcal{C}(\text{SNR}, \beta = 1) = \log_2(\text{e})$. Thus, given P sufficient to waterfill over all available eigenmodes, the per-receive antenna approximation error magnitude is upper-bounded by $\log_2(\text{e})$ scaled by $1/\zeta_s$ as in (84). □

As evidenced by Propositions 3 and 4, we witness an interesting interplay between the error upper bound and the actual error observed. On the one hand, using fewer available eigenmodes increases the value of ζ_s, which in turn decreases the maximum possible error magnitude. On the other hand, using more available eigenmodes brings d_s closer in value to r, which decreases the modeling error. Note that, when all available signal dimensions are utilized by setting $d_s = r$, the original closed-form asymptotic capacity solution is regained. Therefore we expect the largest error for largest $|r - d_s|$, and smallest error both as $d_s \to r$ and $d_s \to 0$.

3.3.5 Computing the MIMOME Secrecy Capacity

To compute the AN generated secrecy capacity for the general MIMOME case, we combine the results of Propositions 1-3. With the approximations for each channel and new set $\mathcal{D}'$ of antenna pairs, the secrecy capacity $\hat{C}^{sec}$ of the MIMOME system can be approximated via

$$\hat{C}^{sec} = \max_{\substack{(d_s,d_a):d_s+d_a\leq t,\ d_s\leq r,\ d_a\geq\lceil\sqrt{et}-d_s\rceil \\ (P_s,P_a):P_s+P_a\leq P}} [r\mathcal{R}^B - e\mathcal{R}^E], \tag{89}$$

The simplicity of this approximation is evident upon comparing with (31). Expectation over random channel gains has been eliminated and replaced with closed-form expressions, and the optimization method of choice can be implemented over a smaller search space. Even if the result is non-convex, the results can be used to intelligently select initial conditions to efficiently search the space with gradient descent methods. However, because of the great reduction in computation, exhaustive search becomes a quite reasonable approach.

While most capacity calculations are done offline during the system design phase, it is still advantageous to have easy-to-compute expressions for capacity for several reasons. First, with the proposed expressions, an eavesdropper will be able to quickly bound the secrecy rate of the main channel. If the channel is evolving in time, using our proposed expression will greatly reduce the complexity required to make the approximations. But a more compelling case is that these expressions simply make it easier for secrecy researcher to compare the rates achievable with a suggested implementation to the best case rates.

3.4 Results

3.4.1 MIMOME Secrecy Capacity Approximation

To test the accuracy of the approximated secrecy capacity, we compared our results with 10^4 Monte Carlo trials. Figure 9 shows an example of the overall asymptotic secrecy capacity approximation given in (89) for various antenna configurations plotted against the actual ergodic secrecy capacity. Although the approximation combines two large-scale approaches, it nonetheless performs with accurate results for realistic numbers of antennas. For $t = 8$, we tested cases of equal numbers of antennas at Ex and Rx, along with cases where $r > e$ and $e > r$. Performance is good for all configurations, with the exception of the case of $e = 3$ and $r = 5$ for SNR < 5 dB, where the secrecy capacity is overestimated; however, for such low power and rates, AN is unlikely to be an efficient choice of secrecy methods. Note that, for SNRs of interest, the relative error for the case where $e > r$ is smaller than the $r > e$ case; this is due to the decrease in approximation error with decrease in allocated signal dimensions. To further investigate the performance of the overall approximation, we now look at the individual approximation performance for each channel.

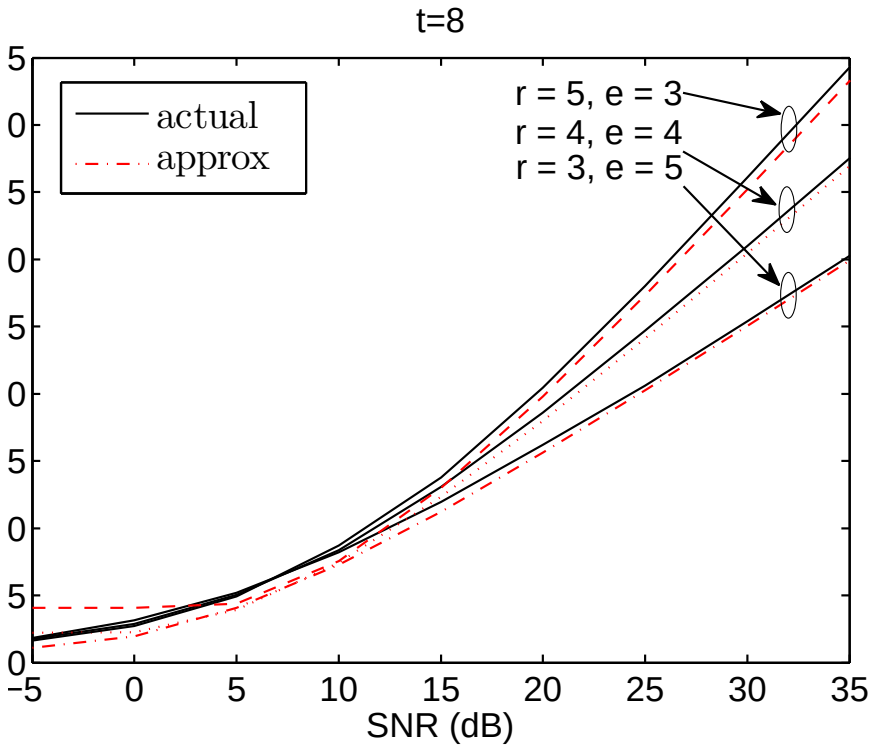


Figure 9: Performance comparison of the large-scale AN secrecy capacity approximation $\hat{R}^{sec}$ to actual secrecy capacity R^{sec} for antenna configurations with realizable numbers.

3.4.2 Eavesdropper Channel Approximation

To investigate the accuracy of the Ex channel approximation, we ran 10^4 Monte-Carlo simulations for various antenna configurations. The minimum guaranteed secrecy capacity is simulated by letting receiver noise at the Ex go to zero, or equivalently by letting the SNR at Ex grow very large. Figure 10 shows the multiuser-interference based approximation for various AN dimensions as a function of SNR. The approximation is shown to be accurate across all values of d_a for high SNR. Since the Ex location is unknown in general, the worst case is assumed to maintain secrecy, and it is only necessary for the approximation to show accuracy in the high-SNR range. Matching results in [21], we see that Eve's ability to mitigate the effects of AN by moving physically closer to the Tx is limited; that is, the Ex capacity grows with SNR for the low SNR but then plateaus at moderate to high SNR.

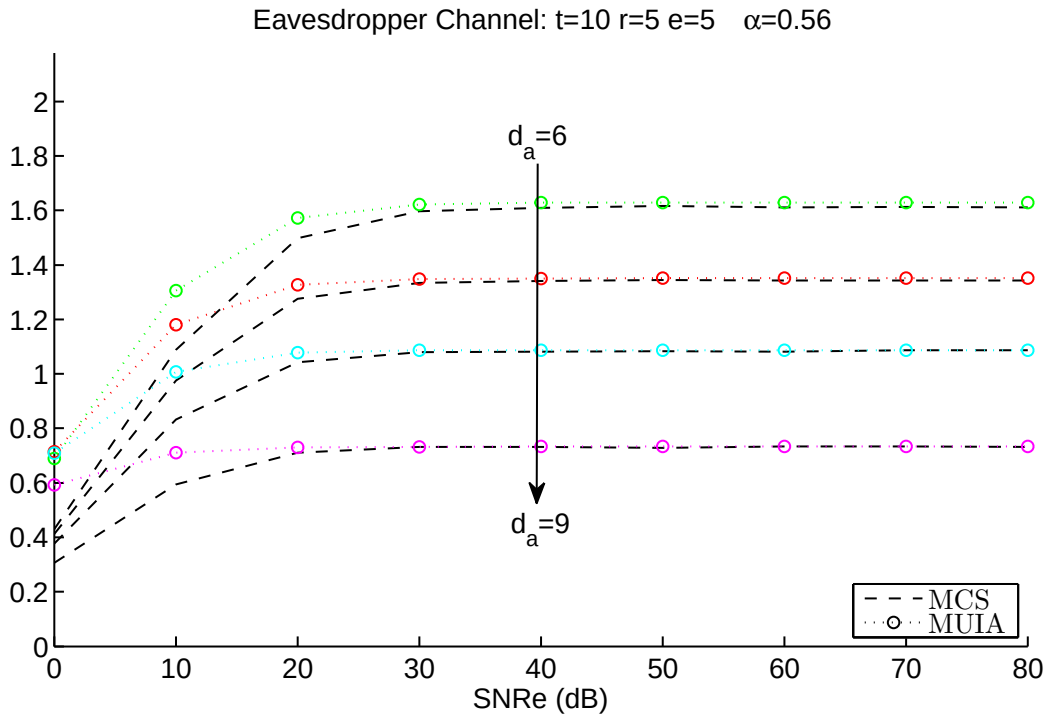


Figure 10: Eavesdropper simulated ergodic capacity (MCS) and large-scale multiuser-interference approximation (MUIA) with respect to power proportion α for the case of high SNR and $\beta = 2$.

In Figure 11 is shown comparison for the low β case plotted versus percentage of power α. The accuracy of the multiuser-interference approximation approach appears largely insensitive to α except at the highest α values, where a slight overestimation occurs. The approximation is tight in the lower ranges of α when signal dimensions are limited. The message symbols are assumed to be unencrypted other than via AN degradation, thus the highest α levels are unlikely to be selected during the maximization over power allocation in (31), and the approximation yields good results for values of interest. Finally, note that approximation error present is an *overestimation* of true value; since the Ex capacity term is subtracted from the main channel capacity to compute secrecy capacity, any error in the Ex capacity term should be overestimation in order to preserve overall security.

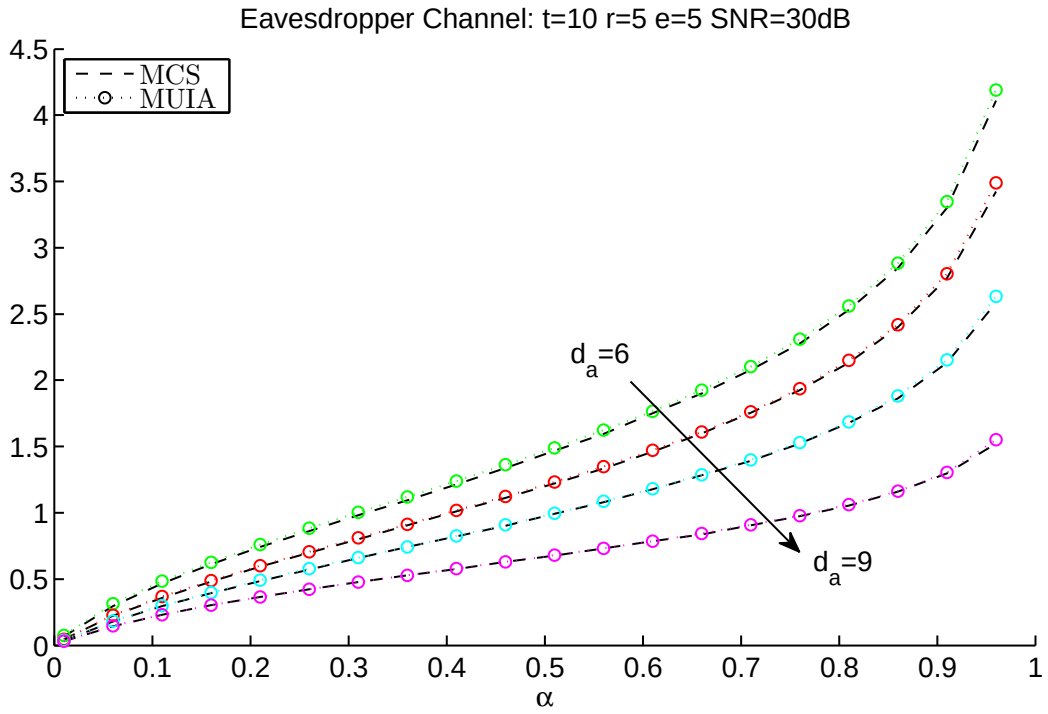


Figure 11: Eavesdropper simulated ergodic capacity (MCS) and large-scale multiuser-interference approximation (MUIA) with respect to power proportion α for the case of moderate SNR and $\beta = 2$.

3.4.3 Main Channel Approximation

For the large-scale MIMO main channel approximation, we again ran 10^4 Monte-Carlo trials for comparison with our novel large-scale MIMO approximation, as well as the partial PDF integration method. In Figure 12 we show the case of $t = 10, r = 5, e = 5$ and SNR $= 35$dB. Approximation error for the main channel is greater than the multiuser-interference approximation. Note that when $d_s = r$, the approximation matches results from Monte-Carlo simulation.

The performance of the main-channel asymptotic approximation is very good for any $\beta \geq 2$. The increase in error for $\beta < 2$ is exemplified in Figures 13 and 17, which show the case of $t = 15$ with $\beta = 1.5$ (or $r = 10$). Both asymptotic approximation curves are displaced even for the case where $d_s = r$. For β values approaching 1, the SNR required for almost sure convergence to the large-scale asymptotic model grows

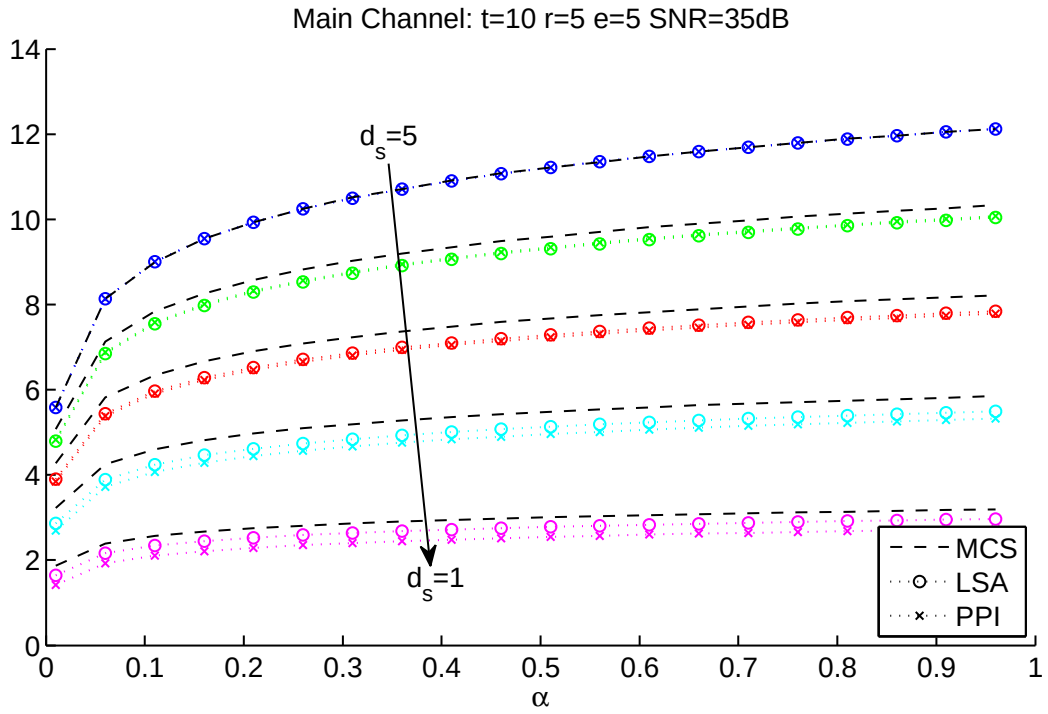


Figure 12: Main channel: ergodic simulation (MCS) compared with large-scale asymptotic approximation (LSA), and partial PDF integration (PPI) for $\beta = 2$.

large[85] and a different formulation is needed; for higher β values, the approximation is good for easily attainable SNR levels. If we decrease the number of receive antennas such that $\beta \geq 2$, the asymptotic approximations perform much better, as seen in Figures 14 and 15. Even when the number of antennas at Rx and Ex is as small as 3, the large-scale MIMO approximation is tight for $\beta = 5$. The accuracy appears also to be insensitive to power allocation α.

For $\beta \geq 2$ and sufficient SNR, performance of both approximation methods is very good. When $d_s = r$ and all signal dimensions are utilized, we observe that both approximation methods yield results identical to Monte-Carlo simulation. Despite the fact that both approximation methods model large antenna configurations, we see both perform well for realistic antenna numbers. Remarkably, the closed-form heuristic solution outperforms the numerical integration technique for the tested cases, and the difference is more apparent as number of signal dimensions decreases. This

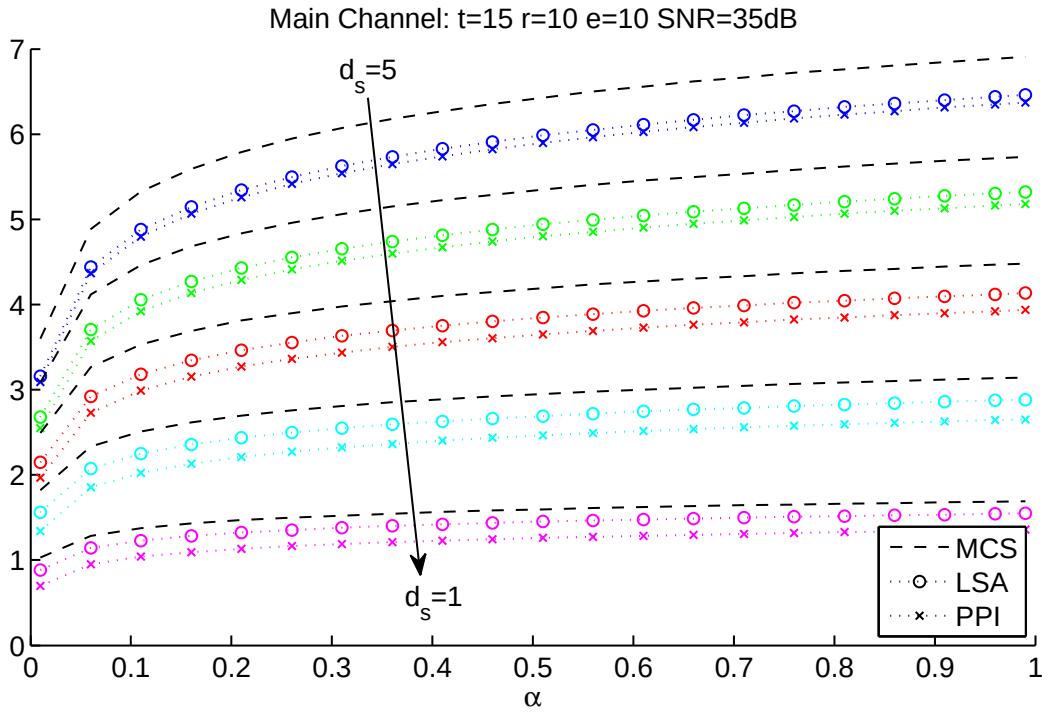


Figure 13: Main channel: ergodic simulation (MCS) compared with large-scale asymptotic approximation (LSA), and partial PDF integration (PPI) for $\beta = 1.5$.

effect is due to the decreasing bounded error as $d_s \to 0$.

Figures 16 and 17 show the percentage error as a function of SNR. Error values for successively lower signal dimensions show successively higher error percentages, as expected since the approximation is made by reducing the number of eigenmodes used.However, at high (very high) SNR the error is less than around 10% (5%) of the total, and the resulting dramatic decrease in complexity from the closed-form expression may justify their use. Note that for all d_s, SNR, and α values of interest, the approximations *underestimate* the main channel capacity. Analogously with overestimation in eavesdropper approximation, underestimation error in the main channel is critical to maintaining security.

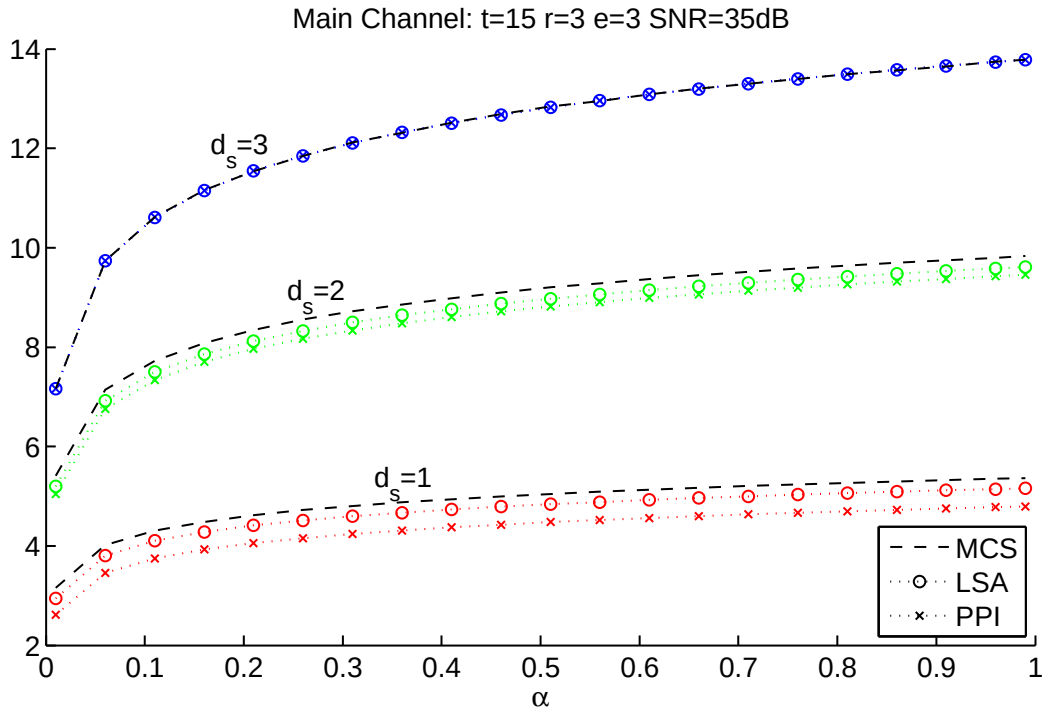


Figure 14: Main channel: ergodic simulation (MCS) compared with large-scale asymptotic approximation (LSA), and partial PDF integration (PPI) for $\beta = 5$.

3.4.4 Complexity Reduction

One primary objective is to provide a low-complexity implementation of secrecy capacity. In the past, floating-point operations (FLOPS) were used as a metric for measuring the computational complexity of an algorithm. With the advent of parallel processing and multi-core processors, FLOPS are no longer a viable measure of complexity, since algorithms that are highly parallelized can sometimes be computed more quickly than those that are not, even with higher FLOP counts. In fact, MathWorks has removed the functions for FLOPS-counting from its standard MATLAB package, and replaced it in documentation with suggestions for simple execution time calculations [57].

Nonetheless, it is important to note in certain cases how FLOPS might (or might not) scale with increases in antennas. As an example comparison, consider the well

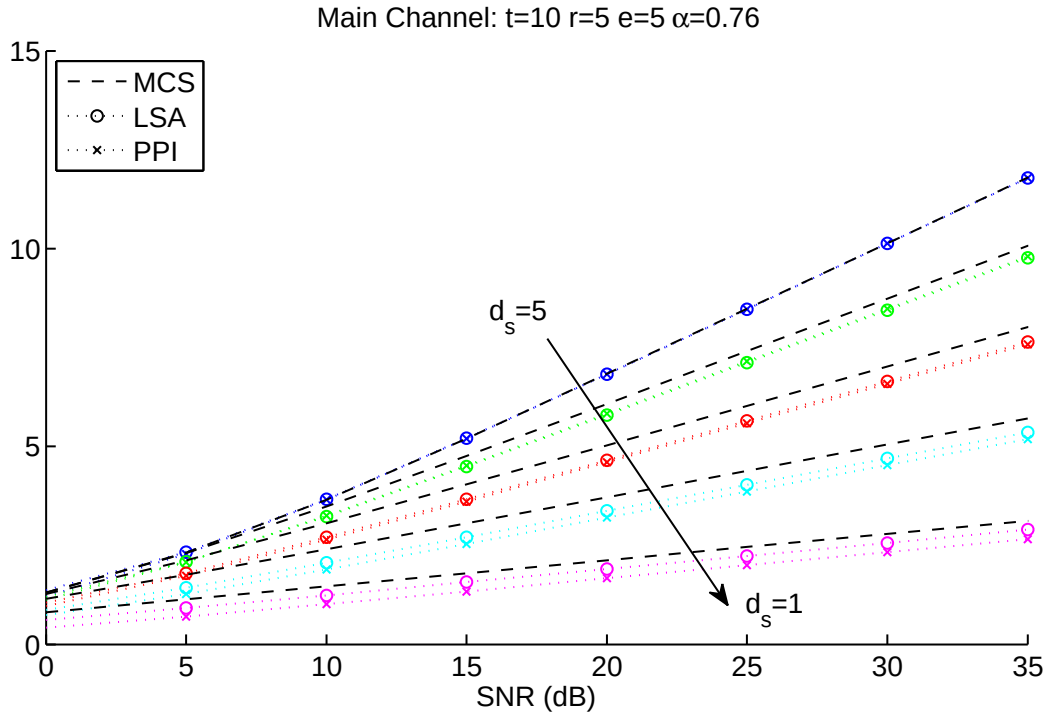


Figure 15: Main channel: ergodic simulation (MCS) compared with large-scale asymptotic approximation (LSA), and partial PDF integration (PPI) for $\beta = 2$.

known log-det formula for simulating main-channel capacity (i.e. the first term in (34)). Depending on the algorithm used, the number of FLOPS required to compute a matrix determinant for a $p \times p$ matrix can range from approximately $\mathcal{O}(p^2)$ on upwards to $\mathcal{O}(p^4)$. The large-scale MIMO closed-form approximation given here has equivalent complexity (in order of magnitude) regardless of matrix size.

As an example, we ran two sets of Monte-Carlo trials on a computer equipped with a 32-bit dual-core Intel processor. The results of these experiments are shown in Tables 2 and 3 for the eavesdropper and main channels, respectively. For the eavesdropper channel, we have used the MATLAB function 'fzero' to solve (55) for η_1 and (56) for η_2 at each iteration. With this method, the multiuser approximation showed a reduction of two orders of magnitude.

As expected with a closed-form solution, the reduction in computation time for the main channel was even more dramatic, at six orders of magnitude less than the

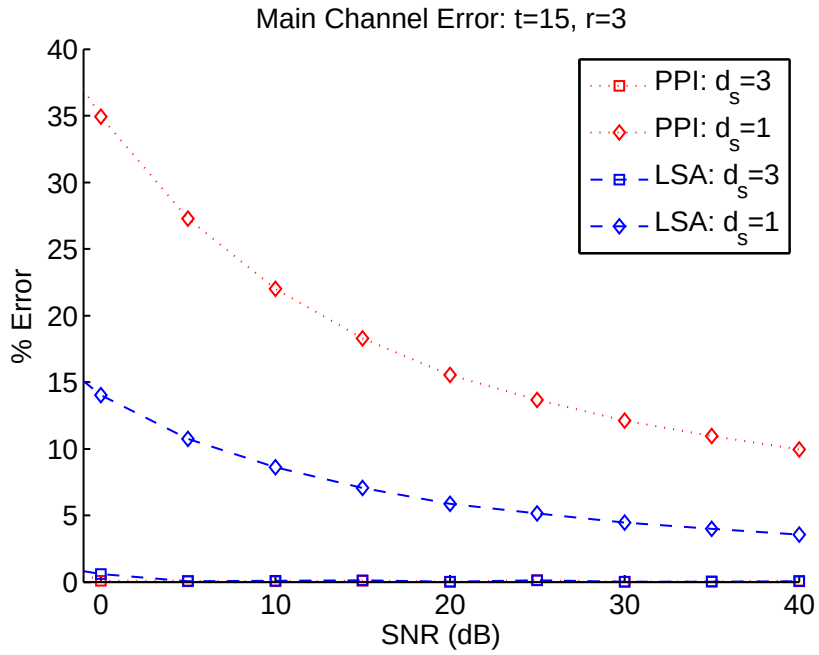


Figure 16: Main channel: percentage error in large-scale asymptotic approximation (LSA), and partial PDF integration (PPI) for the case of $\beta = 5$.

10^4 Monte-Carlo trials. Thus, while the main channel approximation may produce modest amounts of error, the enormous reduction in computation time may make its use worthwhile, and enable its use in resource-constrained wireless systems. The computation time required for the PPI approximation is also shown; the large-scale approximation we present here is consistently favorable three by orders of magnitude in this comparison as well.

Table 2: Eavesdropper channel computation times for Monte-Carlo simulation (MCS) trials, and multiuser interference approximation (MUIA).

t	e	MCS (s)	MUIA (s)
10	3	4.7×10^2	7.1
10	8	1.0×10^3	15.7
15	3	6.0×10^2	9.6
15	10	1.7×10^3	18.1

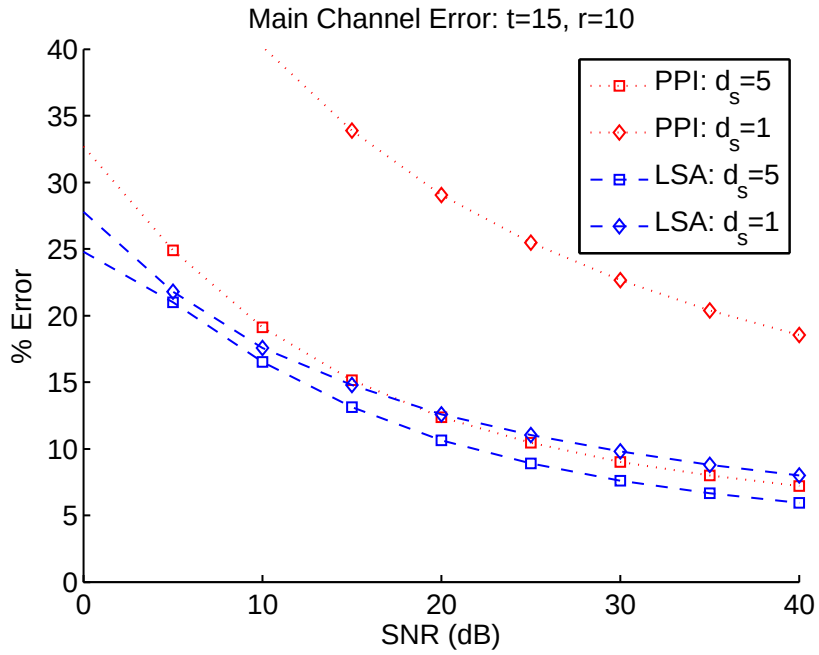


Figure 17: Main channel: percentage error in large-scale asymptotic approximation (LSA), and partial PDF integration (PPI) for the case of $\beta = 1.5$.

3.5 Discussion

While an exact closed-form solution to the AN generated secrecy capacity is an intractable problem for the MIMOME channel, we have demonstrated that asymptotic approximations can be used effectively in place of ergodic Monte-Carlo simulation to accurately estimate the secrecy capacity in an AN system with Tx-Rx antenna ratio over a wide range of SNR. In doing so, the computational complexity involved can

Table 3: Main channel computation times for Monte-Carlo simulation (MCS) trials, Large-Scale Approximation (LSA), and Partial PDF Integration (PPI).

t	r	MCS (s)	LSA (s)	PPI (s)
10	3	1.8×10^{3}	4.7×10^{-4}	4.3×10^{-1}
10	8	1.8×10^{3}	3.2×10^{-4}	2.6×10^{-1}
15	3	4.2×10^{3}	7.6×10^{-4}	5.3×10^{-1}
15	10	6.5×10^{3}	7.6×10^{-4}	5.2×10^{-1}

be enormously reduced, potentially by many orders of magnitudes. This complexity reduction would allow for comparison of the specific implementation with secrecy capacity in complexity constrained or adaptive systems with some expected channel evolution. The approximation methods presented here maintain secrecy by providing a lower bound on available secrecy rates for SNRs of interest. The eavesdropper-channel rate approximation method is seen to perform with near exactness with the worst-case assumption of infinite SNR, while the main-channel approximation error magnitude was shown to be bounded. Finally, though simulated here for the i.i.d. Gaussian channel model, the techniques we present require no such assumption and are generalizable to any MIMOME channel with i.i.d. entries of arbitrary distribution.

Chapter IV

JOINT RADAR-COMMUNICATION SYSTEM IN DOUBLY SELECTIVE CHANNELS

In Chapters 2 and 3, we presented tools useful in interference design. In this chapter, we consider interference in the design process. As the prevalence of wireless technologies continues to grow, the spectrum becomes increasingly crowded. Hence, interference between systems operating in the same frequency band and at the same time is also an increasingly important issue. This chapter investigates the performance of a cooperative, jointly-designed communication-radar system. At the core of this investigation is the notion that, despite major differences in overall mission, the processes involved in radar detection mirror those of channel estimation in a communication system in many ways. By cooperating, the redundant processing can be shared and interference reduced.

If both systems operate independently, in overlapping frequency bands, and without regard to the other, interference is unavoidable. The most straightforward solution to eliminate interference is to divide the resources available into separate regions of time or frequency through policy, such as the Federal Communications Commission (FCC) spectral allocation or dynamic spectrum access [20, 104]. In an environment where it is desired to operate both radar and communication systems, this amounts to either the systems taking turns using the whole frequency band or allocating two non-overlapping portions of the band for simultaneous operation. Here, we explore the possibility of dividing neither time nor frequency; our system allows both systems to share the entire available spectrum at all times.

4.1 Introduction

In a frequency-selective channel, the transmitted signal is spread in time, causing inter-symbol interference which must be corrected for at the receiver. If the receiver does not know the channel *a priori*, it is common to devote a portion of the transmitted signal to training (i.e. pilot) symbols. PSAM is a popular choice for pilot symbols, and is able to capture time-domain channel variations by spreading the pilot symbols throughout a transmission block [9, 13]. Radar uses repeated pulses like those in PSAM to identify Doppler shifts induced by moving targets [68]. While the goals of radar and communication are inherently different, both require characterization of the multipath channel; that is, both systems require a channel estimate. Radar systems use the channel estimate to detect and locate targets, whereas communications systems use the estimate to account for the effects of fading. This forms the basis for our joint radar-communication system, where a single channel estimation process is shared between the two systems.

We assume the multipath environment is doubly-selective, i.e., the channel varies over both frequency and time. Further, we design our transmit signal so that the received signal can be easily decomposed into data-only and training-only signals. This decouples the channel and data estimation processes. In the decoupled system, we allocate a portion of power to estimate the channel and use the remainder to transmit data. For a block transmission scheme with decoupled linear estimation, equipowered and equispaced training symbols have been shown to be both the minimum mean-square error (MMSE) and maximum-capacity (lower bound) strategy [49]. We begin with this equipowered and equispaced single-pulse strategy, which has been shown to be optimal for communication. Because radar detection requires more energy than channel estimation for communication, this optimal scheme may not be feasible to implement using actual radar amplifiers. To explore more practical solutions, we consider suboptimal training schemes with energy spread over multiple consecutive

pulses. In particular, we compare the capacity lower bound from optimal training with those achieved using Barker sequences.

The combination and/or cooperation of radar and communication is not a new topic. Previous studies have primarily addressed either waveform design or radar-communication coexistence issues (i.e. interference mitigation). The joint operation we study in this chapter requires full cooperation between the radar and communication in both waveform design and hardware. The problem setup is illustrated in Figure 18. To highlight the contributions of our work, we enumerate the following features of our chosen configuration:

- One single-antenna transmitter shared by radar and communication systems,
- One transmitted signal vector consisting of both data and pilot symbols,
- Narrowband transmission,
- One single-antenna, shared receiver ,
- One received signal vector, which is distributed to each system after reception for independent processing,
- Elimination of interference in the time domain,
- One (at least) mobile terminal.

Since we design our one transmitted signal for both systems, both systems share the full spectrum at all times. In contrast to previous works that propose dividing the available spectrum between systems (e.g. [36, 83, 91]), our joint design *capitalizes* on redundancy between channel estimation and radar detection by allowing both systems to use the same training signal. Our single antenna transmission design is desirable in that it is low complexity, helps keep hardware costs low, and is more applicable to the predominant existing hardware; however, it preempts use of MIMO techniques such

as the orthogonal waveform interference mitigation in [16], or multiple-access channel models as in [5]. We also show that a narrowband approach is effective, in contrast to wideband or ultra-wideband techniques in [16, 83, 70]. With the time-selective channel model we use, OFDM techniques such as those used in [17, 81, 77, 46] are likely to experience interference from spectral leakage, and system performance may suffer. We employ a basis-expansion model to capture the variations of the channel in both time and frequency domains. In [17], Barker sequences for pulse-compression (other sequence choices for pulse-compression and their effects are considered in [80]); in contrast, here we use Barker sequences for their autocorrelation and sidelobe properties and to reduce peak-to-average power ratio (PAPR), and our implementation has no spreading effect on the transmit spectrum.

Finally, the majority of previous studies assume monostatic radar that uses a portion of its transmit signal (or bandwidth) to communicate to a separate receiver that is uninterested in the radar signal. In contrast, we assume the bistatic case where the receiver is both interested in the data sent by the transmitter and detecting targets in the multipath environment. Rather than dividing time or spectrum between the two systems, we keep the bandwidth and structure of the waveform constant while dividing the total power between data and pilot symbols. The bistatic radar model we use significantly complicates Doppler calculations. For a comprehensive treatment of bistatic clutter and bistatic Doppler derivations, respectively, see [94, Ch. 11] and [93, Ch. 5].

Notation: Bold-face capital (lower-case) letters denote matrix (vector) values, and plain text denotes scalar values. Superscript $^{\mathrm{H}}(^{\mathrm{T}})$ denotes the Hermitian (regular) transpose, and superscript * is used for conjugation. $\lfloor\cdot\rfloor$ is the integer floor. $\mathrm{E}[\cdot]$ denotes expectation. The trace of a matrix is denoted $\mathrm{tr}[\cdot]$. We use $\|\cdot\|$ to denote the Euclidean norm of a vector, and $\otimes$ to denote the Kronecker product. We use $\mathrm{diag}[\mathbf{x}]$ to denote a square matrix with vector $\mathbf{x}$ as its diagonal elements and zeros elsewhere.

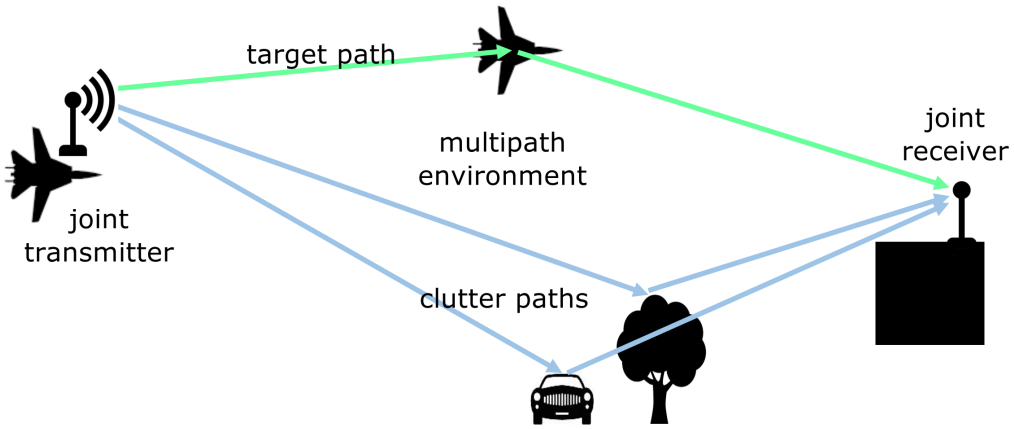


Figure 18: Problem setup. The joint system uses a single antenna at both the mobile transmitter and stationary receiver, and designs a single waveform to be used by both the wireless communication and bistatic radar systems.

4.2 System Model

4.2.1 Doubly-Selective Channel Model

The impulse response of a doubly-selective channel varies with time parameter t and delay parameter τ. Let the time and delay-varying channel impulse response be $h(t;\tau)$. The scattering function

$$S_h(f;\tau) \triangleq \int_{-\infty}^{\infty} A_h(\Delta t;\tau) \mathrm{e}^{-j2\pi f \Delta t} d\Delta t \tag{90}$$

describes the average output power of the channel for Doppler frequency f and delay τ, where

$$A_h(\Delta t;\tau) \triangleq \mathrm{E}\left[h^*(t;\tau)h(t+\Delta t;\tau)\right] \tag{91}$$

is the 2-D autocorrelation function with respect to time shift Δt. The average and root-mean-square delay spreads are found using the standard definitions in [24, Ch. 3]. We assume $|S_h(f;\tau)| \approx 0$ for $|\tau| > \tau_{max}$ and $\forall\, f$, and $|S_h(f;\tau)| \approx 0$ for $|f| > f_{max}$ and $\forall\, \tau$. For a given channel, the values of τ_{max} and f_{max} are easily measured empirically, and thus assumed to be known. We assume the channel remains constant for some duration NT_s, where T_s is the sampling period at the receiver and N is a positive

integer. This model invites block-based processing, where a contiguous block of N transmitted symbols is processed concurrently.

We use a Fourier basis expansion model (BEM) to capture the multipath delay and Doppler characteristics of the channel. With knowledge of f_{max} and τ_{max}, the channel can be represented with $L+1$ delay samples and $Q+1$ Doppler samples where $L = \lfloor \tau_{max}/T_s \rfloor$ and $Q = \lceil f_{max}/\Delta f \rceil$, $1/\Delta f = NT_s$, and where Δf is the Doppler sample spacing. Therefore all multipath reflections arrive within L delay samples after the pulse, with a Doppler-sample between $-Q/2$ and $Q/2$. Let i denote the received sample index, and define the block index $k = \lfloor i/N \rfloor$. Using the BEM, each $h(i;l)$ is defined by its Fourier coefficients $h_q(k;l)$ to capture the time-selectivity of the channel:

$$h(i;l) = \sum_{q=0}^{Q} h_q(k;l) \mathrm{e}^{j\omega_q i} \qquad \forall\ l \in \{0, L\}, \tag{92}$$

where

$$\omega_q \triangleq \frac{2\pi}{N}(q - Q/2) \tag{93}$$

is the q^{th} frequency component.

We also assume that $h(i;l) = c(i;l) + s(i;l)$ is the summation of clutter, $c(i;l)$, and target $s(i;l)$. Similar to $h(i;l)$, the BEM expands $c(i;l)$ and $s(i;l)$ as

$$c(i;l) = \sum_{q=0}^{Q} c_q(k;l) \mathrm{e}^{j\omega_q i}, \tag{94}$$

$$s(i;l) = \sum_{q=0}^{Q} s_q(k;l) \mathrm{e}^{j\omega_q i}, \tag{95}$$

where $c_q(k;l)$ and $s_q(k;l)$ are the Fourier coefficients of the k^{th} block for the clutter and target, respectively. Each $c_q(k;l)$ is an independent, but not identically distributed, zero-mean circularly-symmetric complex Gaussian random variable with variance $\sigma^2_{c_q(k,l)}$. We assume the target is a Swerling I point target [68] independent

of all clutter. Let l_0 and q_0, respectively, denote the delay bin and Doppler basis of the target. Then the sum in (95) simplifies to

$$s(i;l) = \alpha(k)\delta(l-l_0)\mathrm{e}^{j\omega_{q_0} i}, \tag{96}$$

where $\alpha(k) \sim \mathcal{CN}(0, \sigma_\alpha^2)$ is the effective complex target gain that incorporates the target radar cross section (RCS).

4.2.2 Block Transmission Model

As stated in Section 4.2.1, the channel model invites block-based processing. Define $\mathbf{u}_k$ as the kth transmitted block vector. Our transmission scheme is the same as [49], which breaks $\mathbf{u}_k$ into M subblocks. The first and last L symbols in the training portion of each subblock are set to zero (i.e. zero-padded), which prevents the returns from the information and training portion of the subblocks from interfering with each other. Further, this ensures there is no interference between blocks or between subblocks within a block. While it is also possible to decouple equally effectively by using a cyclic prefix, zero-padding is more power efficient since all transmitted cyclic prefix symbols are discarded at the receiver. This training strategy, therefore, effectively decouples channel estimation from symbol decoding.

The motivation for designing decoupled signaling is to reduce decoding complexity at the receiver. In general, estimating the channel and transmitted data is a nonlinear estimation problem (see e.g. [87, 82]). By padding the space between information symbols and the training symbols with L zeros, the problem splits into two separate linear estimation problems by simply selecting the appropriate samples at the receiver.

Since our assumed design eliminates inter-block interference (IBI), and since we will process each received block in an identical manner, we hereafter focus on one block and omit the block index k. Therefore, we may write the transmit sequence as

$$\mathbf{u} = [\mathbf{d}_1^{\mathrm{T}}\ \mathbf{b}_1^{\mathrm{T}}\ \mathbf{d}_2^{\mathrm{T}}\ \mathbf{b}_2^{\mathrm{T}}\ \ \ldots\ \mathbf{d}_M^{\mathrm{T}}\ \mathbf{b}_M^{\mathrm{T}}]^{\mathrm{T}}, \tag{97}$$

where $\mathbf{d}_m$ is the m^{th} data subblock and $\mathbf{b}_m$ is the m^{th} training subblock. With this transmission scheme, the ith received sample is

$$y(i) = \sum_{l=0}^{L} h(i;l)u(i-l) + w(i), \tag{98}$$

where $w(i)$ is zero-mean circularly-symmetric complex Gaussian with variance σ_w^2. In matrix-vector form, the received block is

$$\mathbf{y} = \mathbf{H}\mathbf{u} + \mathbf{w}, \tag{99}$$

where $\mathbf{y} = [y(1) \dots y(N)]^{\mathrm{T}}$ and $\mathbf{w} = [w(1) \dots w(N)]^{\mathrm{T}}$. Defining

$$\mathbf{D}_q = \mathrm{diag}[1 \ \mathrm{e}^{j\omega_q} \ \dots \ \mathrm{e}^{j\omega_q(N-1)}], \tag{100}$$

the Fourier-basis channel expansion is

$$\mathbf{H} = \sum_{q=0}^{Q} \mathbf{D}_q \mathbf{H}_q. \tag{101}$$

Each $\mathbf{H}_q$ is a lower-triangular $N \times N$ Toeplitz matrix with first column $[h_q(0) \ \dots \ h_q(L) \ \mathbf{0}_{1\times(N-L)}]^{\mathrm{T}}$ and first row $[h_q(0) \ \mathbf{0}_{1\times(N-1)}]$. Note that for any q, the Fourier coefficients are functions only of delay τ, and the time-selectivity of the channel is described in the frequency domain.

Define the block data symbol vector $\mathbf{d} \triangleq [\mathbf{d}_1^{\mathrm{T}} \ \mathbf{d}_2^{\mathrm{T}} \ \dots \ \mathbf{d}_M^{\mathrm{T}}]$ and the block training vector $\mathbf{b} \triangleq [\mathbf{b}_1^{\mathrm{T}} \ \mathbf{b}_2^{\mathrm{T}} \ \dots \ \mathbf{b}_M^{\mathrm{T}}]^{\mathrm{T}}$, and let $\bar{N}_m^d$ and $\bar{N}_m^b$ denote the length of the mth data and training subblocks, respectively. The total number of data and training symbols are then $N_d = \sum_{m=1}^{M} \bar{N}_m^d$ and $N_b = \sum_{m=1}^{M} \bar{N}_m^b$, respectively. The symbols arriving at the receiver only as a result of training symbols (i.e., the portion of the received signal containing no multipath delay from data symbol transmission) are $\mathbf{y_b} = \mathbf{H_b}\mathbf{b} + \mathbf{w_b}$, which are easily extracted from $\mathbf{y}$ by simply selecting the rows with indices corresponding to integers on the interval $[r_1^b, r_2^b]$, where

$$r_1^b = (m-1)(\bar{N}_m^d + \bar{N}_m^b) + \bar{N}_m^d + L + 1 \tag{102}$$

$$r_2^b = m(\bar{N}_m^d + \bar{N}_m^b), \tag{103}$$

for each $m \in [1, M]$. We may write $\mathbf{y_b} = [(\mathbf{y}_0^b)^{\mathrm{T}}\ (\mathbf{y}_1^b)^{\mathrm{T}}\ \ldots\ (\mathbf{y}_{M-1}^b)^{\mathrm{T}}]^{\mathrm{T}}$, where

$$\mathbf{y}_m^b = \mathbf{H}_m^b \mathbf{b}_m + \mathbf{w}_m^b, \tag{104}$$

the portion of the channel matrix that only affects the m^{th} subblock is $\mathbf{H}_m^b = \sum_{q=0}^{Q} \mathbf{D}_{q,m}^b \mathbf{H}_{q,m}^b$, $\mathbf{w}_m^b$ contains the noise samples for the training portion of the m^{th} subblock, and $\mathbf{H}_{q,m}^b$ and $\mathbf{D}_{q,m}^b$ are the submatrices of $\mathbf{H}_q$ and $\mathbf{D}_q$ due to the training portion of the m^{th} subblock, respectively. Expanding the pilot-only signal across both Fourier bases and subblock index, we have

$$\begin{aligned}
\mathbf{y_b} &= \sum_{q=0}^{Q} \mathbf{D}_q^b \mathbf{H}_q^b \mathbf{b} \\
&= \sum_{q=0}^{Q} \begin{bmatrix} \mathbf{D}_{q,1}^b \mathbf{H}_{q,1}^b \mathbf{b}_1 \\ \vdots \\ \mathbf{D}_{q,M}^b \mathbf{H}_{q,M}^b \mathbf{b}_M \end{bmatrix} \\
&= \sum_{q=0}^{Q} \begin{bmatrix} \mathbf{D}_{q,1}^b \mathbf{B}_1 \\ \vdots \\ \mathbf{D}_{q,M}^b \mathbf{B}_M \end{bmatrix} \mathbf{h}_q,
\end{aligned} \tag{105}$$

where the last equality of (105) follows from the commutativity of convolution ($\mathbf{H}_{q,m}^b \mathbf{b}_m = \mathbf{B}_m \mathbf{h}_q$). By expanding the sum over Q, we can write the received training signal in vector matrix form as

$$\mathbf{y_b} \triangleq \mathbf{\Phi_b} \mathbf{h} + \mathbf{w_b}, \tag{106}$$

where $\mathbf{\Phi_b}$ is a *known* block matrix with $[\mathbf{\Phi_b}]_{m,q} = \mathbf{D}_{q,m} \mathbf{B}_m$, $\mathbf{h}_q \triangleq [h_q(0)\ \ldots\ h_q(L)]^{\mathrm{T}}$, and $\mathbf{h} = [\mathbf{h}_0^{\mathrm{T}}\ \mathbf{h}_1^{\mathrm{T}}\ \ldots\ \mathbf{h}_Q^{\mathrm{T}}]^{\mathrm{T}}$.

4.3 System Performance

Define the total power transmitted as

$$P \triangleq \mathrm{E}[\|\mathbf{u}\|^2], \tag{107}$$

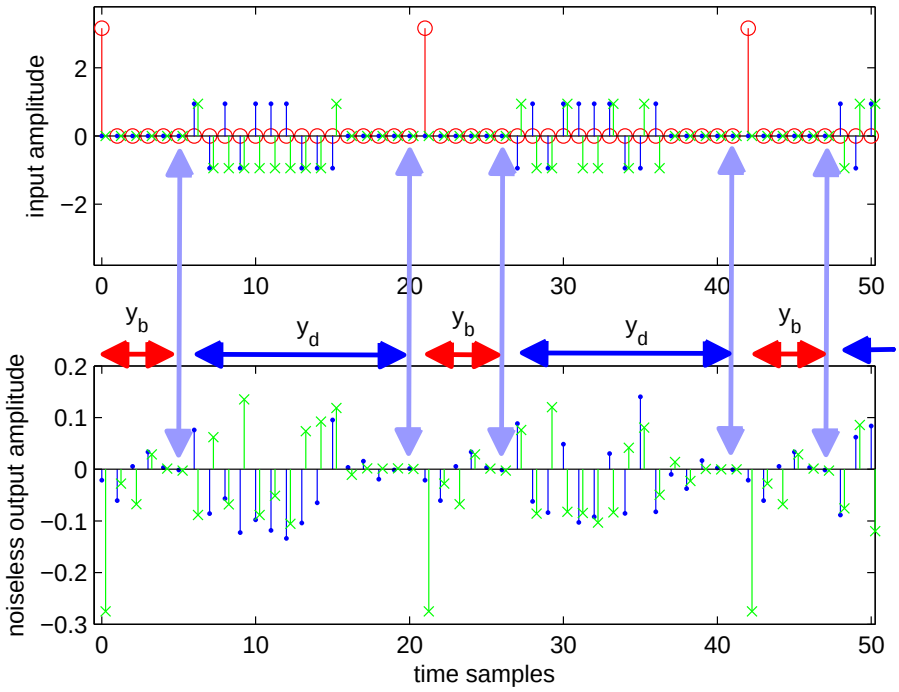


Figure 19: Subblock structure of an example transmit waveform using optimal training (top) and the resulting noise-free channel output (bottom), for channel length 5 and data subblock length 10. Red circles show the single training symbol per subblock. Blue dots and green x's show the real and imaginary parts of the data symbols using QPSK modulation. Vertical arrows match the end of the zero padding regions (top) with corresponding spots where received channel energy returns to zero. Horizontal arrows indicate the partitioning of the received (noise-free) signal into data and training.

which is split between power allocated to data symbols ($P_d \triangleq \mathrm{E}[\|\mathbf{d}\|^2]$) and training symbols ($P_b \triangleq \|\mathbf{b}\|^2$). To quantify the effect of sharing power between systems, we define the power allocation parameter ρ such that $P_d \triangleq \rho P$ and $P_b \triangleq (1-\rho)P$. Denote the average power per data and training symbol, respectively, as $\bar{P}_d = P_d/N_d$ and $\bar{P}_b = P_b/N_b$. Further, define $\mathbf{H_d}$ as the portion of the channel matrix affecting only data symbols and $\mathbf{y_d} = \mathbf{H_d d} + \mathbf{w_d}$ as the resulting received signal; these can be formed by selecting from $\mathbf{H}$, $\mathbf{y}$ and $\mathbf{w}$ the rows with indices corresponding to integers

on the interval $[r_1^d, r_2^d]$, where

$$r_1^d = (m-1)(\bar{N}_m^d + \bar{N}_m^b) + 1 \tag{108}$$

$$r_2^d = (m-1)(\bar{N}_m^d + \bar{N}_m^b) + \bar{N}_m^d + L, \tag{109}$$

for each $m \in [1, M]$ and column indices on the intervals $[c_1^d, c_2^d]$, where

$$c_1^d = (m-1)(\bar{N}_m^d + \bar{N}_m^b) + 1 \tag{110}$$

$$c_2^d = (m-1)(\bar{N}_m^d + \bar{N}_m^b) + \bar{N}_m^d, \tag{111}$$

for each $m \in [1, M]$.

4.3.1 Radio Optimization

4.3.1.1 LMMSE Channel Estimation

For a given channel realization, the channel capacity is a function of the transmitted power and random channel gains. Averaging over the channel realization yields the ergodic capacity

$$\overline{C} \triangleq \frac{1}{N} \mathrm{E}\left[\log\det\left(\mathbf{I} + \frac{\bar{P}_d}{\sigma_w^2}\mathbf{H_d}\mathbf{H_d}^{\mathrm{H}}\right)\right] \text{ bits/s/Hz}, \tag{112}$$

where expectation is over random channel gains $\mathbf{H_d}$ (i.e. the parts of $\mathbf{H}$ contributing to $\mathbf{H_d}$). The overbar notation signifies that $\overline{C}$ represents an *upper bound* on capacity since $\mathbf{H_d}$ is unknown and must be estimated. Since no channel information is assumed known at the transmitter, (112) implicitly assumes uniform power allocation (i.e. $\mathrm{E}[\mathbf{d}\mathbf{d}^{\mathrm{H}}] = \bar{P}_d\mathbf{I}$). This upper bound provides a benchmark for performance with channel estimation. The LMMSE channel estimate is [38, 49]

$$\hat{\mathbf{h}} = \frac{1}{\sigma_w^2}\left(\mathbf{R}_\mathbf{h}^{-1} + \frac{1}{\sigma_w^2}\mathbf{\Phi}_\mathbf{b}^{\mathrm{H}}\mathbf{\Phi}_\mathbf{b}\right)^{-1}\mathbf{\Phi}_\mathbf{b}^{\mathrm{H}}\mathbf{y}, \tag{113}$$

where $\mathbf{R_h} = \mathrm{E}[\mathbf{h}\mathbf{h}^{\mathrm{H}}]$. The corresponding mean square error (MSE) is

$$\epsilon_{\mathrm{MMSE}} = \mathrm{tr}\left[\left(\mathbf{R}_\mathbf{h}^{-1} + \frac{1}{\sigma_w^2}\mathbf{\Phi}_\mathbf{b}^{\mathrm{H}}\mathbf{\Phi}_\mathbf{b}\right)^{-1}\right]. \tag{114}$$

If $\mathbf{R_h}$ is diagonal, the MSE in (114) is minimized by designing the product $\mathbf{\Phi_b}^H\mathbf{\Phi_b}$ to be diagonal [60, App. I]. This can be seen intuitively by noting that $\mathbf{\Psi} \triangleq \mathbf{\Phi_b}^H\mathbf{\Phi_b}$ is positive definite, and by the Hadamard inequality the diagonal terms $[\mathbf{\Psi}]_{i,i}$ are at a maximum when $\mathbf{\Psi}$ is diagonal; thus, the trace of the inverse is minimized under the same condition.

The formula for the capacity of a channel is a function of its random channel gains, and does not traditionally account for effects of channel estimation. However, poor channel estimation will surely result in lower achievable rates. Note that $\mathbf{y}_b$ is not a function of the estimation error. To incorporate the effect channel estimation error has on communication rates, we use the lower bound capacity from [49]:

$$\underline{C} \triangleq \frac{1}{N}\mathrm{E}\left[\log\det\left(\sigma_w^2\mathbf{I} + \bar{P}_d\mathbf{R}_\mathbf{v}^{-1}\hat{\mathbf{H}}_\mathbf{d}\hat{\mathbf{H}}_\mathbf{d}^{\mathrm{H}}\right)\right] \text{ bits/s/Hz}, \tag{115}$$

where $\hat{\mathbf{H}}_\mathbf{d}$ is the estimate of $\mathbf{H_d}$, $\mathbf{R_v} \triangleq \bar{P}_d\mathrm{E}[\tilde{\mathbf{H}}_\mathbf{d}\tilde{\mathbf{H}}_\mathbf{d}^{\mathrm{H}}] + \sigma_w^2\mathbf{I}$, and $\tilde{\mathbf{H}}_\mathbf{d} \triangleq \hat{\mathbf{H}}_\mathbf{d} - \mathbf{H_d}$. The expectation in (115) is again over random channel realizations $\mathbf{H_d}$, but also the noise $\mathbf{w_d}$; the estimates $\hat{\mathbf{H}}_\mathbf{d}$, and hence error matrices $\tilde{\mathbf{H}}_\mathbf{d}$, are functions of $\mathbf{H_d}$ and noise $\mathbf{w_d}$. At high signal to noise ratio (SNR), the LMMSE estimate that results in maximal lower bound on ergodic channel capacity is attained [49] if:

C1. all data subblocks have the same number of symbols (i.e. $\bar{N}_1^d = \bar{N}_2^d = \cdots = \bar{N}_M^d \triangleq \bar{N}_d$),

C2. all training subblocks have only one nonzero symbol (i.e. $\bar{N}_1^b = \bar{N}_2^b = \cdots = \bar{N}_M^b \triangleq \bar{N}_b = 2L+1$) and are allocated equal power (i.e. $\|\mathbf{b}_m\|^2 = P_b/M$ for each $m \in [1, M]$), and

C3. the number of subblocks equals the number of Doppler bases (i.e. $M = Q+1$).

Given aformentioned C1-3, the identical structure of subblocks can be exploited to write the error covariance matrix as

$$\mathrm{E}[\tilde{\mathbf{H}}_\mathbf{d}\tilde{\mathbf{H}}_\mathbf{d}^{\mathrm{H}}] = \mathbf{I}_M \otimes (\mathrm{E}[\tilde{\mathbf{H}}_{\mathbf{d},m}\tilde{\mathbf{H}}_{\mathbf{d},m}^{\mathrm{H}}]), \tag{116}$$

where $\tilde{\mathbf{H}}_{\mathbf{d},m}$ is the portion of $\tilde{\mathbf{H}}_{\mathbf{d}}$ found by taking rows and columns defined in (108)-(109) and (110)-(111), respectively. Noting that the error covariance is diagonal, the subblock error covariance can be written as

$$\mathrm{E}[\tilde{\mathbf{H}}_{\mathbf{d},m}\tilde{\mathbf{H}}_{\mathbf{d},m}^{\mathrm{H}}] = \begin{bmatrix} \mathbf{V}_1 & & \\ & \epsilon_{\mathrm{MMSE}}\mathbf{I}_{N-L} & \\ & & \mathbf{V}_2 \end{bmatrix}, \tag{117}$$

where $\mathbf{V}_1$ and $\mathbf{V}_2$ are diagonal matrices of size $L \times L$ with entries

$$[\mathbf{V}_1]_{k+1,k+1} = \sum_{l=0}^{k}\sum_{q=0}^{Q}\mathrm{E}[\tilde{h}_q(l)\tilde{h}_q^*(l)], \tag{118}$$

$$[\mathbf{V}_2]_{k+1,k+1} = \sum_{l=k+1}^{L}\sum_{q=0}^{Q}\mathrm{E}[\tilde{h}_q(l)\tilde{h}_q^*(l)], \tag{119}$$

for $k \in [0, L-1]$, where $\tilde{h}_q(l) = h_q(l) - \hat{h}_q(l)$. For *optimal* training, the transmit vector resulting from conditions C1-3 is of the form

$$\mathbf{u} = [\mathbf{d}_1^{\mathrm{T}}\ \mathbf{0}_{1\times L}^{\mathrm{T}}\ b\ \mathbf{0}_{1\times L}^{\mathrm{T}}\ \ldots\ \mathbf{d}_M^{\mathrm{T}}\ \mathbf{0}_{1\times L}^{\mathrm{T}}\ b\ \mathbf{0}_{1\times L}^{\mathrm{T}}]^{\mathrm{T}}, \tag{120}$$

where $b = P_b/M$.

4.3.1.2 Least-Squares Channel Estimation

The LMMSE channel estimate assumes that the channel covariance matrix is known. There are instances, such as a sudden shift in environment, where this assumption is unwarranted. We can lower bound the achievable communication rates by removing the known channel statistics and using data-driven least-squares (LS) channel estimation. The least-squares channel estimate is [73]

$$\hat{\mathbf{h}}_{\mathrm{LS}} = \left(\mathbf{\Phi}_{\mathbf{b}}^{\mathrm{H}}\mathbf{\Phi}_{\mathbf{b}}\right)^{-1}\mathbf{\Phi}_{\mathbf{b}}\mathbf{y}_{\mathbf{b}}. \tag{121}$$

Note that $\hat{\mathbf{h}}_{\mathrm{LS}} \sim \mathcal{CN}(\mathbf{h}, \sigma_w^2 \left(\mathbf{\Phi}_\mathbf{b}^{\mathrm{H}} \mathbf{\Phi}_\mathbf{b}\right)^{-1})$, so the least-squares estimation error is

$$\epsilon_{\mathrm{LS}} \triangleq \mathrm{tr}\left[\sigma_w^2 \left(\mathbf{\Phi}_\mathbf{b}^{\mathrm{H}} \mathbf{\Phi}_\mathbf{b}\right)^{-1}\right] \tag{122}$$

$$= \sum_{l=0}^{(Q+1)(L+1)} \frac{1}{\left[\frac{1}{\sigma_w^2} \mathbf{\Phi}_\mathbf{b}^{\mathrm{H}} \mathbf{\Phi}_\mathbf{b}\right]_{l,l}} \tag{123}$$

$$\geq \sum_{l=0}^{(Q+1)(L+1)} \frac{1}{\left[\mathbf{R}_\mathbf{h}^{-1}\right]_{l,l} + \left[\frac{1}{\sigma_w^2} \mathbf{\Phi}_\mathbf{b}^{\mathrm{H}} \mathbf{\Phi}_\mathbf{b}\right]_{l,l}} = \epsilon_{\mathrm{MMSE}}, \tag{124}$$

where (123) follows from conditions C1-3, and the inequality in (124) follows from the fact that $\mathbf{R}_\mathbf{h}$ is a covariance matrix with all diagonal elements greater than or equatl to zero. There is no direct link between LS estimation error in (122) and LS estimate (121) and the capacity bound in (115). However, since the lower bound proof in [49, App. C] relies on an assumption of high SNR, and since at high SNR the LMMSE and least-squares estimates converge, the effect of the channel estimates on the lower bound capacity is negligible. Thus, minimizing $\mathbf{R}_\mathbf{v}$ (by plugging in the errors of LS estimates) can maximize the lower bound capacity with LS approximation.

4.3.2 Radar Target Detection

We can decompose the pilot portion of the received signal in (106) into its clutter and target components:

$$\mathbf{y}_\mathbf{b} = \mathbf{\Phi}_\mathbf{b}\mathbf{s} + \mathbf{\Phi}_\mathbf{b}\mathbf{c} + \mathbf{w}_\mathbf{b} \tag{125}$$

$$= \mathbf{\Phi}_\mathbf{b}\mathbf{s} + \tilde{\mathbf{w}}, \tag{126}$$

where $\mathbf{c} = [c(0) \ldots c(L)]^{\mathrm{T}}$, $\mathbf{s} = [s(0) \ldots s(L)]^{\mathrm{T}}$, and $\tilde{\mathbf{w}} \triangleq \mathbf{\Phi}_\mathbf{b}\mathbf{c} + \mathbf{w}_\mathbf{b}$ with covariance

$$\mathbf{R}_{\tilde{\mathbf{w}}} = \mathrm{E}[(\mathbf{\Phi}_\mathbf{b}\mathbf{c} + \mathbf{w}_\mathbf{b})(\mathbf{\Phi}_\mathbf{b}\mathbf{c} + \mathbf{w}_\mathbf{b})^{\mathrm{H}}]. \tag{127}$$

The detection problem then becomes

$$\mathcal{H}_0 : \mathbf{y}_\mathbf{b} = \tilde{\mathbf{w}} \tag{128}$$

$$\mathcal{H}_1 : \mathbf{y}_\mathbf{b} = \mathbf{\Phi}_\mathbf{b}\mathbf{s} + \tilde{\mathbf{w}}, \tag{129}$$

where the null hypothesis $\mathcal{H}_0$ represents the case where the received signal is clutter and noise only, and the alternative hypothesis $\mathcal{H}_1$ represents the presence of a target in clutter and noise. The Neyman-Pearson (NP) [39] detector decides $\mathcal{H}_1$ if the likelihood ratio test (LRT) statistic exceeds a threshold:

$$\gamma < \frac{p(\mathbf{y}|\mathcal{H}_1)}{p(\mathbf{y}|\mathcal{H}_0)}. \tag{130}$$

The detection performance when $\mathbf{s}$ is a known vector is easily found. However, from (96) it is clear that both the magnitude and the phase of the target return are unknown quantities. Whether or not the target magnitude $|\alpha(k)|$ is known has no effect on the structure of the detector; thus $|\alpha(k)|$ can be assumed known when deriving the detector, and accounted for using noncoherent integration [68, Ch. 6.2]. Knowing the phase $\angle\alpha(k)$ requires knowing the range to the target to incredible precision, since only a change of a quarter wavelength causes a complete reversal of phase in the returned signal. To account for this unknown phase, we use envelope detection assuming the magnitude is a known vector $\mathbf{m}$, and examine detection performance when $\mathbf{s} = \mathrm{e}^{j\theta}\mathbf{m}$, where $\theta \sim \mathcal{U}(0, 2\pi)$. The probability of detection for a Swerling I target is then [68, Ch. 6.3]

$$P_D = \exp\left[\frac{-\mathcal{T}'}{1+\chi}\right], \tag{131}$$

where $\mathcal{T}'$ is a threshold selected to give a desired probability of false alarm P_{FA} (i.e. $\mathcal{T}' = \mathcal{T}'(P_{FA})$), and χ is the signal to interference (clutter) plus noise ratio (SINR). Note that (131) is monotonic in χ. Using the Cauchy-Schwarz inequality, it is straightforward to show that the maximum SINR achievable is

$$\chi = \mathbf{s}^{\mathrm{H}}\mathbf{\Phi}_{\mathbf{b}}^{\mathrm{H}}\mathbf{R}_{\tilde{\mathbf{w}}}^{-1}\mathbf{\Phi}_{\mathbf{b}}\mathbf{s}. \tag{132}$$

If we assume $\mathbf{R}_{\tilde{\mathbf{w}}}$ is diagonal (i.e. each $c_q(k,l)$ is independent), optimal training signals are used, and the target is a point target, then, using the definitions in (94)-(96), the

SINR in (132) simplifies to

$$\chi = \frac{\sigma_\alpha^2 P_b}{\sigma_{c_{q_0}(k,l_0)}^2 P_b + \sigma_w^2}. \tag{133}$$

Note that (133) is monotonic in P_b. Thus, both the radar performance and the communications performance are tied to the proportion of transmit power allocated to channel estimation. The performance of both systems is considered jointly over P_b in the next section.

Since the two systems fully cooperate, it is theoretically possible to use the entire transmit waveform for detection after the communication system has finished decoding the data. However, we omit the use of data symbols for detection for the following reasons. First, this chapter focuses on low-complexity linear approach. Second, the latency resulting from decoding the data before sending to the radar system would likely be unsatisfactory in many radar applications. Finally, feedback paths in hardware design are generally frowned upon due to timing and synchronization issues. We therefore leave detection using the entire waveform for future work.

4.3.3 Optimality Considerations

When finding an optimal solution, it is important to make explicit *in what sense* a solution is optimal. At the outset we adopted a training scheme shown to be optimal for communication systems; however, other training schemes may perform better for radar purposes because of the higher energy required. In what follows, we will continue to refer to the training scheme that achieves the LMMSE channel estimate as "optimal," while acknowledging that other training schemes may perform better on other metrics.

4.3.3.1 Suboptimal Training

For radar, probability of detection is a function of the total amount of transmitted energy reflecting off the target, rather than the peak transmission power. Using

the repeated single pulse optimal for communication, the peak power required for detection may greatly exceed the capability of amplifiers standard in radar hardware. Instead, the optimal signaling structure can be relaxed to allow the total power needed to detect targets to be distributed over multiple consecutive training symbols.

Barker sequences [25] have two properties that make them a good choice for spreading power allocated to training over multiple symbols: 1) they are constant modulus, facilitating amplification, and 2) they exhibit autocorrelation sidelobes with maximum power inversely proportional to the code length, and therefore provide a good approximation to a single-pulse train. The Barker sequences we employ here differ from Barker coding traditionally used in radar for pulse compression in that the chip duration is equivalent to the symbol duration, so the bandwidth is equivalent for any Barker (as well as optimal) sequence length. Rather than increasing bandwidth, sequences of increasing length instead produce longer overall block lengths. This allows fair comparison of differing sequence lengths, since the capacity lower bound is normalized by block length.

Note that the data symbol subblocks are unaffected by the use of Barker sequences, since we apply them only to training. However, using Barker sequences the lower bound on capacity in (115) is likely to suffer, since a larger percentage of *time* is spent on training. This effect is shown in Figure 20. In addition to total time spent transmitting training symbols, suboptimal training also affects channel estimation error, since Barker sequences have good (but not ideal, like a single optimal training pulse) autocorrelation properties. Using Barker sequences also affects the probability of detection. From (133), it is apparent that sequence length has no effect on probability of detection in the radar system if the clutter plus noise covariance is uncorrelated, and so long as $\mathbf{\Phi}^{\mathrm{H}}\mathbf{\Phi}$ is diagonal. Despite their desirable autocorrelation properties, however, Barker sequences do not produce a strictly diagonal $\mathbf{\Phi}^{\mathrm{H}}\mathbf{\Phi}$, so we must revert to (132) when calculating SINR. We expect that the use of Barker

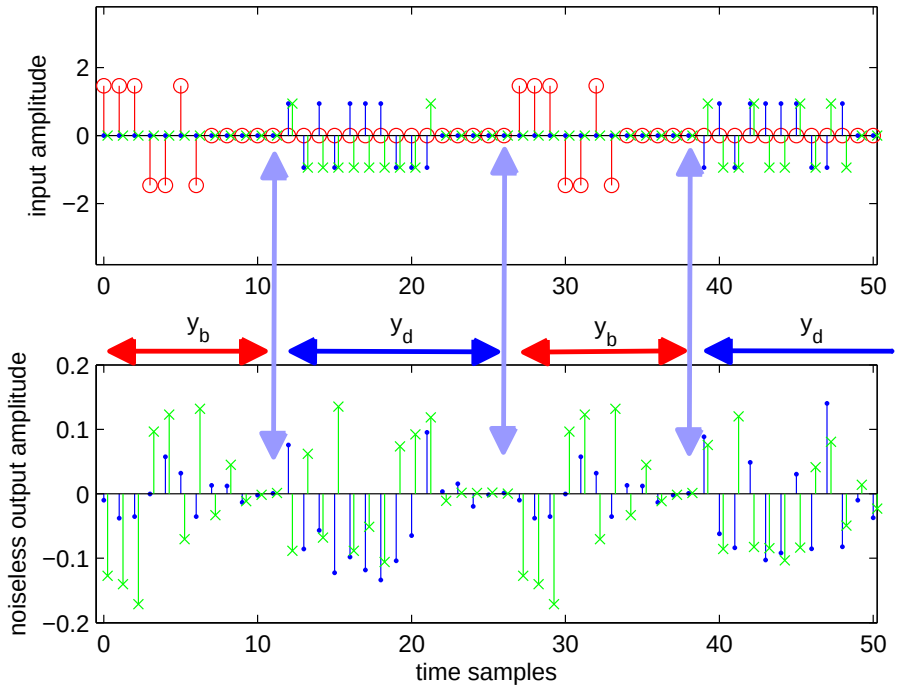


Figure 20: Barker-sequence counterpart to Figure 19. Here, a Barker sequence of length 7 is shown, and all other parameters are held constant. Note the increased length of the received training signal compared to the single-pulse optimal training used in Figure 19.

sequences is likely to have a more detrimental effect on the lower bound on capacity than on probability of detection, since capacity is affected both by time and quality of estimation, whereas the $\mathbf{\Phi}^{\mathrm{H}}\mathbf{\Phi}$ will still be *nearly* diagonal.

4.3.3.2 Sampling Doppler Outside the Clutter Region

For both communication and radar systems, keeping Q to a minimum avoids unnecessary overhead. In communication-only systems, the value is often set to

$$Q = \lceil f_{max} N T_s \rceil \tag{134}$$

so that the highest Doppler frequency sampled coincides with the maximum clutter Doppler component, and the Doppler samples are evenly spaced on the interval $[-f_{max}, f_{max}]$. Here, we use the block length N to be the FFT size used in the BEM.

It has been noted that using a denser FFT and higher Q values can increase the accuracy of the BEM [71]. However, to estimate $Q+1$ Doppler bases we need $Q+1$ subblocks, so increasing Q results in progressively longer block lengths and processing complexity. From a radar perspective, choosing a larger Q may also be required to identify a target producing a Doppler shift that exceeds the maximum Doppler shift produced by clutter. Say, for example, that we are interested in a target with Doppler shift $(1+\delta)f_{max}$, for any $\delta > 0$. Then if we define Q as in (134), our target Doppler will alias. We might then be tempted to accept longer block lengths and increase Q to avoid aliasing, but with the exception of the target Doppler, all Doppler values outside the clutter region are modeled (in Jakes' model) as exactly zero. Thus, $\mathbf{h}$ would become be a *degenerate* Gaussian random vector. While these are interesting issues to be solved, they lie beyond the scope of this chapter. In Section 4.4 we consider cases where the target is located within the Doppler spread of the clutter; the study of targets outside of this spread is left for future work.

4.4 Numerical Examples

We simulated the joint system using 60 Monte Carlo trials. We varied the total block-duration power P in (107) from 20 W to 120 kW, and percentage of power allocated to data over $0 < \rho < 1$. The delay power in our channel was modeled as decaying exponentially as $A_h(0;\tau) = \beta_1 \exp(-\tau/\beta_2)$, with β_1 and β_2 representing the initial power and power decay parameters, respectively. For an exponential decay model with average delay spread μ_τ and RMS delay spread σ_τ, we have $\mu_\tau = \sigma_\tau = \beta_2$. For our simulations we chose β_1 to be 1/10 of the line of sight power at the receiver, and $\beta_2 = 2$ seconds. Figure 21 shows the Doppler power spectrum, normalized such that the total Doppler power sums to 1, and the power delay profile (PDP), normalized by the line of sight power.

We used an initial block size of $N = 2048$, with channel length $L = 30$ and Doppler

resolution $Q = 16$. For our system parameters, we used a carrier frequency of 2 GHz with a bandwidth of 1 MHz; transmit and receive gains of 5 dB; system losses of 2 dB; and a noise figure of 3 dB. Suboptimal training was implemented by simply replacing each scalar b in (120) with an appropriately power-scaled Barker sequence of desired length. For example, if a Barker-4 sequence was used, each b would be replaced with $\frac{\bar{P}_b}{4}[+1, +1, -1, +1]$. To keep the block length N relatively constant, we first set the number of subblocks $M = Q + 1$ and then selected N_d to yield the smallest $N_d + M(2L + L_B) \geq N$, where L_B is the Barker sequence length.

The transmitter and receiver were positioned at $(10, 0)$ km and $(0, 0)$ km, respectively, and the target was positioned at $(5, 7)$ km, as shown in Figure 22. We assumed a stationary transmitter, and mobile receiver and target with instantaneous velocity vectors $(0, -900)$ and $(0, -800)$ km/hr, respectively. With these velocities and positions, the bistatic Doppler shift of the target lies within the total Doppler spread arising from clutter. This allows us to adopt Jakes' model [34] for the channel Doppler spread and find the MMSE channel estimate.

The effect of the power allocation ρ is shown in Figure 23 for the capacity lower bound. The communication system functions well in the lower total power range. Note that the power values given represent fundamentally different quantities: the value given in W or kW is the total power transmitted over the entire block duration; the value in dB is the SNR per symbol at the receiver. The figure shows three curves: the light gray curve is the upper bound from (112) assuming the channel is known perfectly at the receiver and does not require estimation. The solid blue and dotted red curves show the effect of imperfect MMSE and LS estimation, respectively. The left portions of the curves are *power* limited in that there is negligible difference between performance with perfect channel knowledge compared to the estimated channel performance, and rate increases are achieved only by allocating more power to the data signal. The right portions of the curves are *estimation* limited in that the effect of

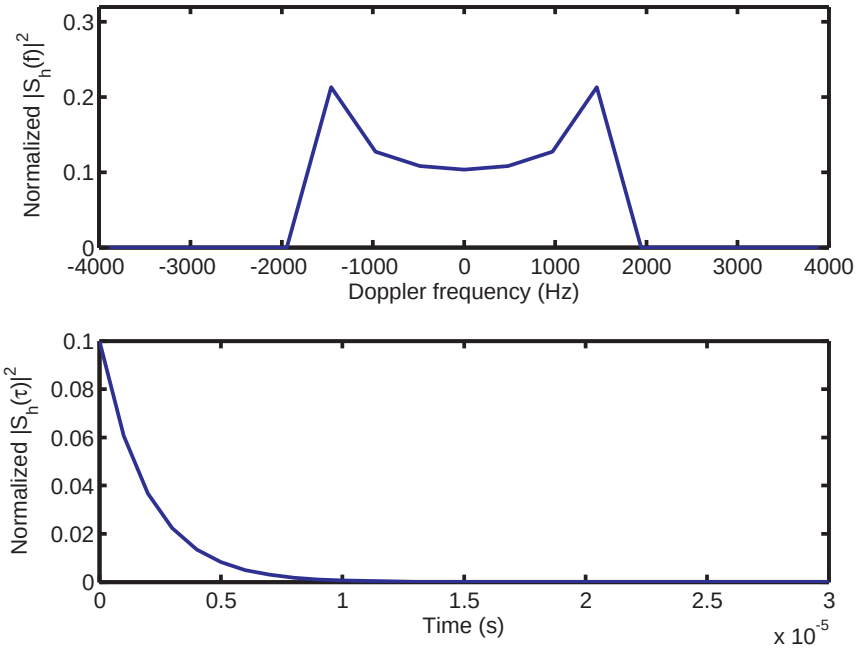


Figure 21: Clutter Doppler power (top) and power delay profile (bottom).

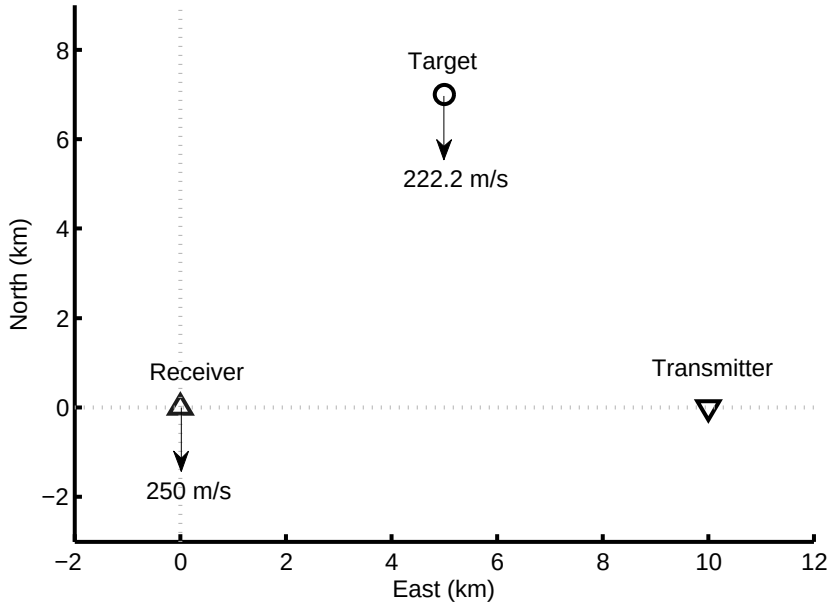


Figure 22: Simulation scenario.

channel estimation becomes salient. These trends appear largely insensitive to overall transmit power across the moderate to high receiver SNR cases tested.

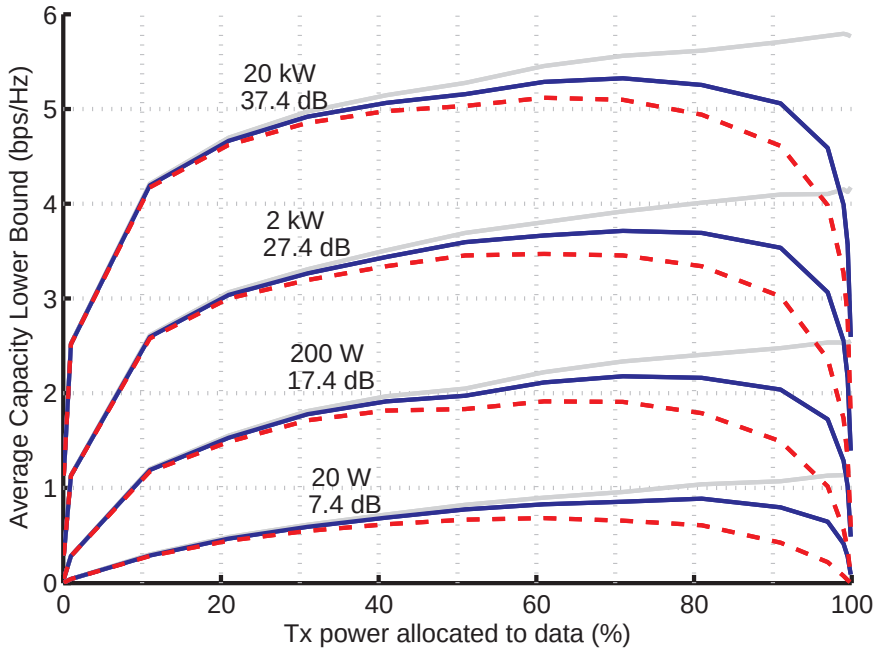


Figure 23: Capacity lower bound as a function of power allocation for various total transmission powers and corresponding receiver SNR per symbol. MMSE: solid blue; LS: dotted red; upper bound: solid light-gray.

The radar detection probability shown in Figure 24 is monotonic in total power allocated to training. For low total power, allocating more power to training greatly increases detection probability, whereas for high total power the benefit of allocating more power to training saturates quickly. Note that the overall power expenditures necessary for the radar system are much higher than those needed for reliable communication. From (131) and (133), it is also clear that detection probability is a function only of the channel realization and total power P_t allocated to training, and thus is unaffected by method of channel estimation so long as optimal training sequences are transmitted. The detection probabilities for Barker sequences show slight performance degradation, but do not significantly change the shapes of the curves. Note that longer Barker sequences actually perform closer to optimal training than shorter ones, since the autocorrelation sidelobes decrease with sequence length.

The joint communication-radar performance is shown in Figure 25. The curves

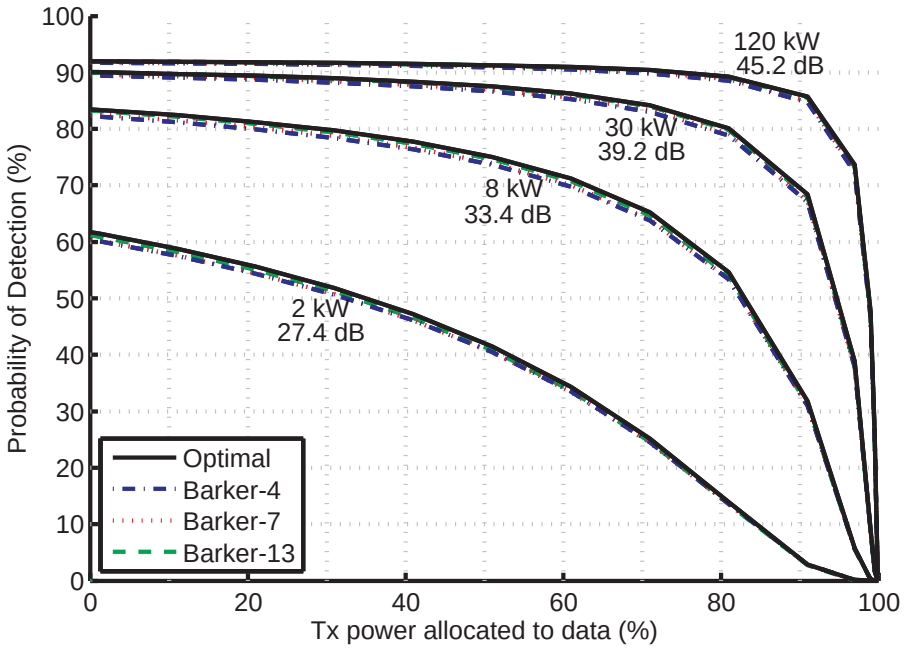


Figure 24: Probability of detection as a function of power allocation for various total transmission powers and corresponding receiver SNR per symbol.

shown are parameterized over $0 < \rho < 1$. Values marked by squares (diamonds) represent the capacity-maximizing values for the MMSE (LS) case. For the MMSE case, the maximizing values for the two lower-power curves are obtained by setting $\rho = 0.71$; for the two higher power curves, the maximizing $\rho = 0.61$. For LS, all maximizing values arise from $\rho = 0.61$. These maximizing values show the diminishing returns of incorporating prior knowledge of channel statistics. We note that the actual achievability region is obtained by dropping a vertical line from the point of maximized capacity lower bound, since anywhere below that point is (unadvisably) achievable simply by selecting an inferior detection method. When total power grows large, inflection points begin to appear in the performance curves. These points indicate the allocation values at which further allocating power away from training becomes more detrimental to detection probability than to the capacity lower bound.

Figure 27 shows the PAPR for blocks using optimal training versus Barker coded training signals. For optimal training, PAPR is monotonically decreasing with power

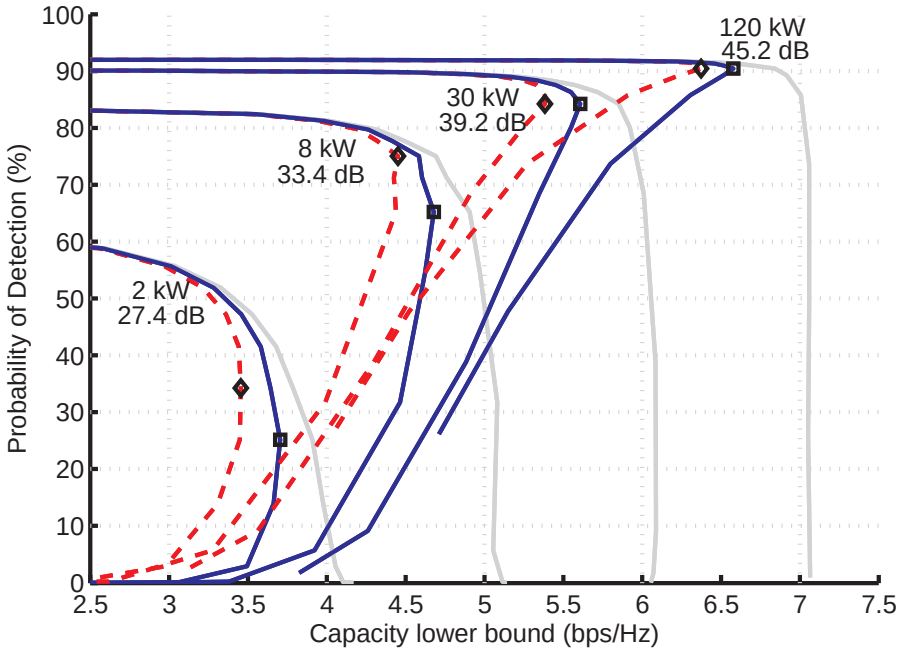


Figure 25: Joint radar-communication system performance for various total transmission powers and corresponding receiver SNR per symbol. MMSE: solid blue; LS: dotted red; upper bound: solid light-gray.

allocated to data. Barker sequences reduce PAPR by up to 10 dB. Codes with length 7 or 13 also achieve the lowest PAPR at lower data allocation values.

Figure 26 shows the time-domain discrete baseband transmitted signal for optimal training versus a Barker code of length 13 for 8 kW total transmit power and $\rho = 0.71$. Even though the power and chosen allocation level are the same for each case, the dynamic range of the optimal training signal is far higher than that of the Barker coded signal, since the optimal training signal concentrates all its power into a single symbol while the Barker code spreads the power over many training symbols. Spreading training energy over multiple symbols could greatly facilitate the amplification process in practical systems.

The effect of using Barker sequences as a suboptimal training scheme is shown in Figures 28 and 29 for the MMSE and LS cases, respectively. In both cases, there is a penalty paid for increasing the length of the nonzero training signal. The penalty

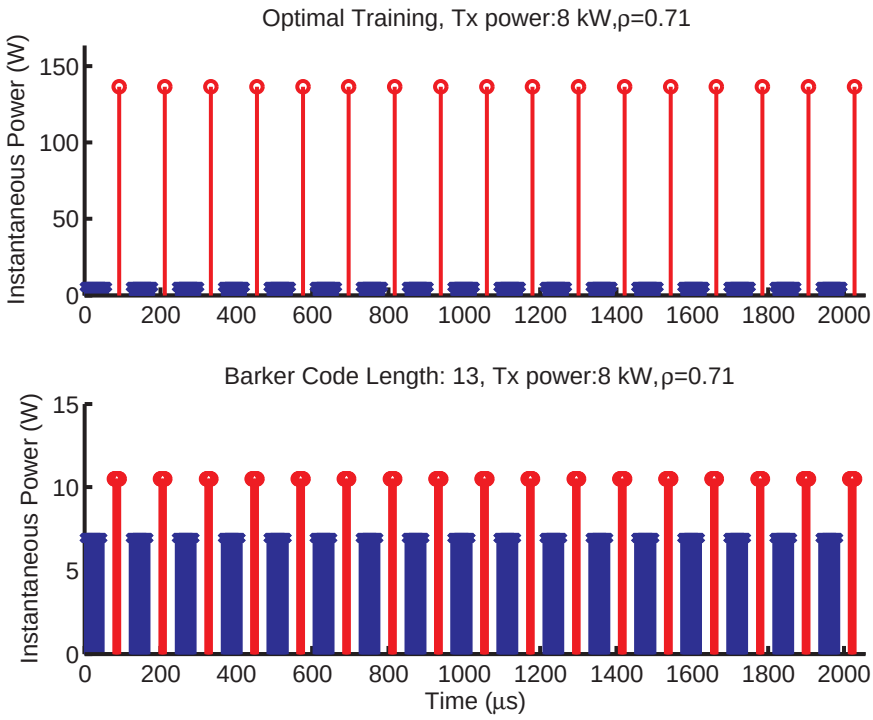


Figure 26: Comparison of training symbol instantaneous power levels using a single pulse per subblock optimal for communications systems (top) and after spreading power among multiple training symbols using a Barker sequence (bottom).

at low SNR is negligible and becomes more substantial as overall transmitted power grows. However, the gaps from the Barker curves to the optimal training curve appear relatively insensitive to allocation level. This signifies that lower bounds on capacity for higher code lengths become *time* limited in that the penalty appears to have little relation to channel estimation quality.

4.5 Discussion

We have presented an analysis framework for a cooperative radar-communication system operating simultaneously in the same frequency band. Our design leverages decoupled training and data to yield low-complexity linear processing for the communication system, and assumes a point-target model, which yields a simple detector structure for the radar system. The specific performance of each system depends on

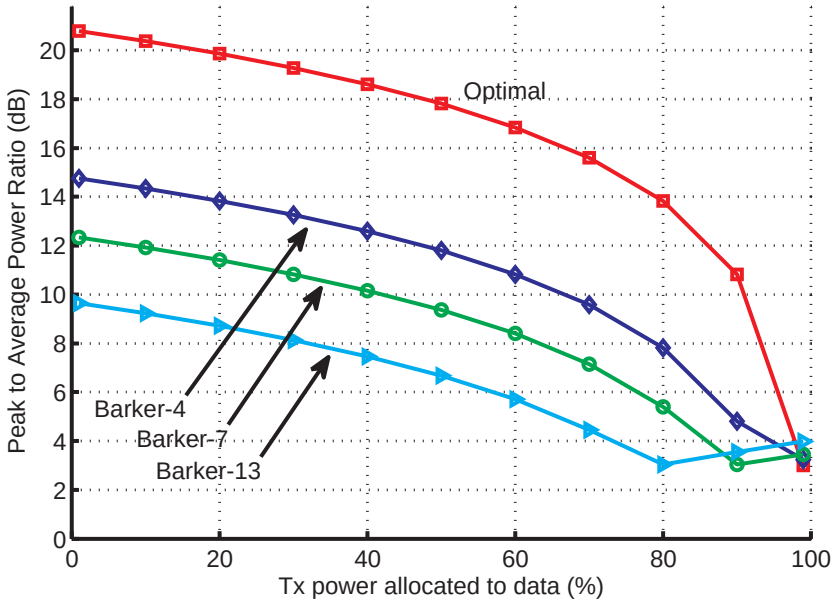


Figure 27: Peak to average power ratio for optimal training and three Barker code training signals.

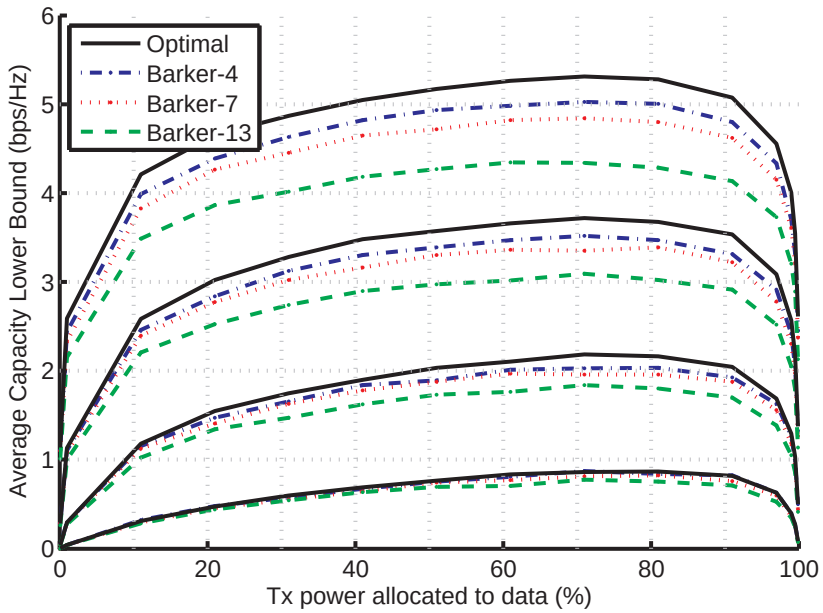


Figure 28: Capacity lower bound using Barker training sequences compared to the optimal training scheme for MMSE channel estimation.

the power allocation, but mutually successful coexistence is possible. Optimal training signals are shown to produce the greatest lower bound on communication rate

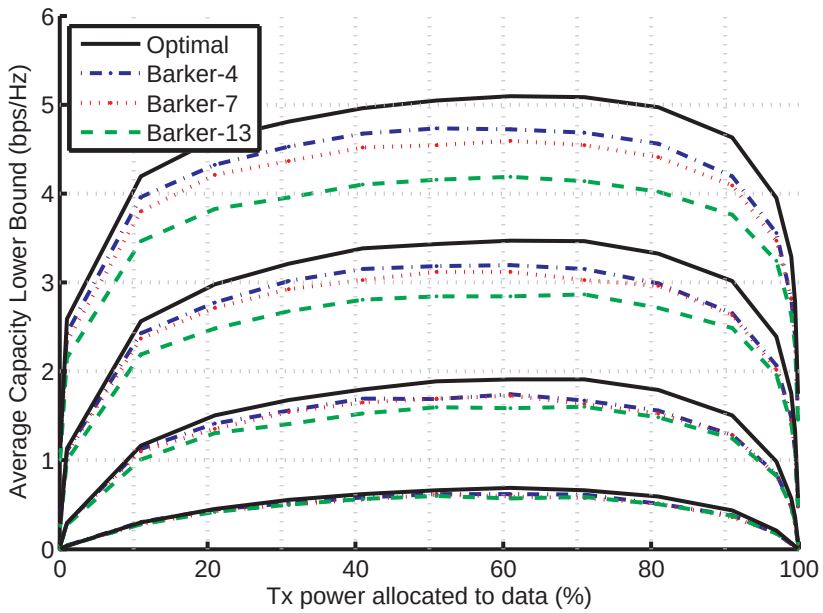


Figure 29: Capacity lower bound using Barker training sequences compared to the optimal training scheme for LS channel estimation.

as well as the maximum probability of detection. Given that amplification is likely to impose real-world constraints on instantaneous transmitted power, we have shown that Barker training sequences are a viable option. The penalty for using Barker sequences is most apparent in the lower bound on achievable communication rate, and less significant for radar detection. Despite being suboptimal, the longer Barker sequences have the advantage of greatly reducing PAPR and retaining near-optimal detection performance. Future work can extend the framework to more more complex scenarios, specifically addressing coupled data and symbol detection with nonlinear processing to compare performance gains with increased complexity, expanding beyond the simplistic point target model, and addressing the possibility of multiple targets.

Chapter V

SECRET WIRELESS COMMUNICATION USING DATA-CARRYING ARTIFICIAL NOISE

In Chapter 4, we saw how interference could be eliminated in the co-design of competing systems. In this chapter, we present a new method of securing communication that combines two previously studied secrecy methods: 1) secret keys, and 2) artificial noise, as detailed in Chapter 3. The new method exploits the randomness property of secret keys that makes encrypted codewords appear noise-like to those who do not posses the key. We leverage this fact to use secret-key encrypted codewords as a form of designed interference. We demonstrate that this new use of intentional interference is simultaneously able to increase achievable secrecy rates and reduce power necessary for a given secrecy rate. We first prove these benefits assuming that there is no cost or overhead associated with using secret keys. We follow the ideal case by examining the more realistic scenario where there is a small price paid for using keys as interference, and give bounds on the achievable rates.

5.1 Introduction

One method of securing wireless communications is symmetric encryption with a secret key at the transmitter (Tx) and decryption with an identical key at the receiver (Rx). Such systems require pre-distribution of keys, and the security they provide is good only so long as the keys themselves are not vulnerable to discovery. In 1949, Claude Shannon published the first framework for the study of secret communication in an information-theoretic sense by proving that a one-time pad (OTP) could perfectly secure communication [75]. Though exceedingly simple in implementation,

Shannon's OTP is limited in applicability because of the strict requirements 1) that the key be at least as long as the message, and 2) that the key be generated from a truly random source. With symmetric keys at both ends of a communication link, the OTP can be implemented quite simply using a (modulo) adder. With such simplicity and the ability to ensure perfect secrecy, it would seem that problem of securing communication would be solved completely.

Unfortunately, OTP encryption is laden with requirements that restrict its practical feasibility for securing wireless communications in most scenarios. First, the key must be random and uniformly distributed over the key space. Second, Shannon showed in 1949 that to ensure perfect secrecy, the length of the secret key must be at least as long as the message itself [76]. Third, any malicious party that intercepts the secret key may immediately decrypt the message. Thus, key distribution itself becomes a security concern: either the key must be generated ahead of time, securely distributed, and securely stored at the Tx and Rx, or must be independently and securely generated by both Tx and Rx. Since generating long and identical strings of truly random symbols at two locations separated in space is not an easy task, the applicability of the OTP has been limited in practice.

The use of the wireless channel for *secret key generation* (SKG) has attracted recent interest. Wireless channels are commonly assumed to be reciprocal, i.e. the multipath properties are identical in both directions of the link between Tx and Rx, and temporal variations of the fading coefficients therefore provide a source of common randomness from which a pair of identical keys can be extracted from various properties of the channel measurements. Due to its ease of measurement, signal amplitude is often used (see, e.g. [62, 54, 99]). SKG methods based on phase differences [28, 72] and time delay (in wideband transmission) [95, 51] have also been studied. Fading channels in rich scattering environments (with no significant line of sight component) are known also to decorrelate quickly in space; distances greater than half

a wavelength are commonly assumed to produce significantly uncorrelated channels [24]. Thus, so long as an eavesdropper (Ex) is not collocated with the Tx or Rx, the channel can be viewed as a source of randomness not only common but also unique to the Tx and Rx.

Key bits can be used as a one-time pad (OTP) to perfectly encrypt communication. Unfortunately, OTP encryption is laden with requirements that restrict its practical feasibility for securing wireless communications in most scenarios. For channels to be perfectly reciprocal, both Tx and Rx must measure the channel simultaneously. Most communications systems are half-duplex, thus in practice measurements at Tx and Rx are not perfectly reciprocal but rather highly correlated. To generate enough randomness to form new key bits, the channel must vary sufficiently in time; keys produced with static terminals, for example, generally have insufficient entropy [35]. Moreover, a channel that varies rapidly may produce sufficient randomness to generate longer key strings, but also decorrelates in time more rapidly, exacerbating the imperfect reciprocity. The available secret key length is the mutual information between the channel estimates [89, 90]. Unfortunately, the amount of key bits that can be extracted from wireless measurements is generally too low to fully encrypt communication with an OTP [14], and varies with the number of multipath reflections [89, 90]. Maximization of the achievable secret key rate has been studied in, e.g. [65, 66].

Alongside opportunistic key generation, another method of secure communications information-theoretically at the physical layer is possible when the SNR of the intended receiver is greater than the SNR of the eavesdropper. Goel and Negi [21, 22] first coined the term *artificial noise* (AN), and showed that a relative SNR advantage could be generated without knowing the exact location of the eavesdropper by transmitting noise in a subspace orthogonal to the main channel. For a detailed exposition of the AN strategy and previous works, refer to Section 3.1. Like SKG, using AN for

secrecy has its own drawbacks. Power efficiency becomes an issue, since power that could be used to transmit information is instead used to transmit AN symbols. Moreover, decomposition of the main channel into orthogonal subspaces requires accurate channel state information at the transmitter (CSIT). Acquiring CSIT is a costly process, both in terms of power and time spent; it is simpler to acquire accurate CSI at the Rx (CSIR) only using, for example, pilot-symbol aided modulation. Channel estimation error at the transmitter not only leaks artificial noise power into the signal space, but also potentially leaks additional signal power towards eavesdroppers.

Inaccuracies in CSI have been previously modeled in primarily two ways: channel quantization and channel perturbation. In [102, 101], CSI is acquired at the Rx and then a quantized version is fed back to the Tx on a rate-limited public channel. Our work differs from [102, 101] first in that CSI is kept secret from outside parties and the Tx and Rx are assumed to undergo a reconciliation process to resolve discrepancies in their estimations (see, e.g. [6]), and second in that the CSI in our model is not constrained to lie in a predefined finite set of matrices. In this chapter, we use a channel perturbation model similar to [58]. However, to derive a robust beamforming technique, [58] assumes that error-free CSIR. We use the perturbation to model channel evolution in time, and therefore we assume that *both* Tx and Rx channel estimates are imperfect. Robust beamforming when the Rx has only a single antenna is considered in [29] and numerical solutions are found. In this manuscript we make no attempt to correct for channel error, but rather acknowledge its existence and quantify its effect on secret communication rates.

5.1.1 Problem Formulation

Secure communication using either SKG or AN requires accurate CSIT. Once the resources have been used to estimate the channel, the information gleaned from the process should ideally be exploited to the greatest extent possible. In this chapter

we show that achievable secrecy rates can be increased beyond the strictly AN case by exploiting of the redundant channel estimation process required by both AN and SKG. Though both SKG and AN have been well explored in previous literature, we know of no previous study that combines the two methods to capitalize upon this redundancy. We call this system *data-carrying artificial noise* (DCAN), since the encrypted symbols exploit the random output properties of an OTP to act as noise, while still carrying information to the legitimate receiver.

The proposed method is as follows. The Tx and Rx exchange training pulses and estimate the channel. From this channel estimate they form a common secret key consisting of a limited number of bits, with which the Tx encrypts none, some, or all of the message symbols using an OTP.[1] Previous studies indicate key rates are generally low compared communication rates. Therefore we focus on the case where only a *portion* of the message symbols can be encrypted. The encrypted symbols are spatially multiplexed with the remaining unencrypted message symbols and AN symbols and transmitted. The intended user has the key and can easily decrypt the encrypted symbols. The output of an OTP is uniformly distributed across the message alphabet, and therefore is unconditionally secure without the key. Thus the encrypted symbols act simultaneously as messages to the Rx and interference to the Ex.

Various studies have been made into the effects of interference in secret communications. Optimal power allocation in a single-antenna 2×2 interference multiple-access channel is examined in [106]. Our work differs from [106] in that we use spatial multiplexing and beamforming in a MIMO system to enhance the effects of interference and generate higher secret communication rates. In this chapter, we assume that

[1]The specifics of the SKG process are beyond the scope of this chapter; A SKG algorithm for fading channels is given in [6], where the Tx and Rx 1) exchange training signals and measure the channel output, 2) perform error correction to reconcile discrepancies between the measurements, and 3) perform privacy amplification [4] through one-way hash functions to ensure the Ex remains ignorant of the final key.

the transmitted symbols will be *nearly* Gaussian, so that the symbols are drawn from a discrete set, but closely approximates Gaussian signaling. With this assumption, the interference acts as Gaussian noise at the Ex. Gaussian noise is known to be most detrimental of all distributions of a given variance [55]. Thus encrypted data symbols can act simultaneously as a information-theoretically secure message to the Rx and as Gaussian noise to Ex.

As with the AN-only case, the DCAN method we introduce in this chapter offers a minimum guaranteed secrecy regardless of SNR at the Ex. The net gain of our proposed scheme can be summarized as follows:

1. Greater information-theoretically secure communication rates, since some secrecy-guaranteeing artificial noise simultaneously transmits information, and

2. Less power (than the AN-only case) required to achieve a desired secrecy rate, since some of the message symbols simultaneously act to confuse anyone intercepting communication that does not possess the secret key.

The outline of this chapter is as follows. Section 5.2 presents the MIMOME system model used throughout the chapter. Section studies the achievable secret communication rates in the case of perfectly known channel stat information (CSI). Section 5.4 derives bounds on secret communication rates assuming that CSI is unknown and must be estimated. The theoretical rates for both cases are illustrated by numerical example in Section 5.5. Finally, conclusions are presented in Section 5.6.

Notation: The following notation is used throughout the chapter. Bold-face lowercase type denotes vector $\mathbf{a}$; bold-face uppercase type denotes matrix $\mathbf{A}$. $|\mathbf{A}|$, $\mathbf{A}^{\mathrm{T}}$, and $\mathbf{A}^{\mathrm{H}}$ are the matrix determinant, transpose, and Hermitian transpose, respectively. The identity matrix of size $p \times p$ is denoted $\mathbf{I}_p$. $\mathbb{C}$ is the field of complex numbers. The entropy of vector $\mathbf{x}$ is $h(\mathbf{x})$; conditional entropy given $\mathbf{z}$ is $h(\mathbf{x}|\mathbf{z})$. The

mutual information between vectors $\mathbf{x}$ and $\mathbf{y}$ is $I(\mathbf{x};\mathbf{y})$; mutual information conditioned on $\mathbf{z}$ is $I(\mathbf{x};\mathbf{y}|\mathbf{z})$. The hat symbol $\hat{a}$ denotes the estimate of value a. $\mathrm{E}_{\chi}[\cdot]$ denotes expectation with respect to the probability distribution on χ, and $\mathrm{cov}(\mathbf{w})$ denotes the covariance matrix of a vector $\mathbf{w}$. We use $\mathrm{diag}(\mathbf{x})$ to mean a matrix with elements of $\mathbf{x}$ along its diagonal and zeros elsewhere; similarly, $\mathrm{diag}(\mathbf{A}_1\ \mathbf{A}_2\ \ldots\ \mathbf{A}_K)$ is a block-diagonal matrix constructed from $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_K$.

5.2 System Model

Define t, r and e as the number of antennas at Tx, Rx, and Ex, respectively. $\mathbf{H} \in \mathbb{C}^{r\times t}$ is the MIMO main (Tx-Rx) channel matrix, and $\mathbf{G} \in \mathbb{C}^{e\times t}$ is the MIMO eavesdropper (Tx-Ex) channel matrices. The pair $(\mathbf{H}, \mathbf{G})$ constitute the MIMOME wiretap channel. We assume a rich-scattering environment, and assume both channels to be flat fading and quasi-static such that the channel is constant for the duration of the channel estimation and subsequent codeword transmission. Thus the entries of $\mathbf{H}$ are independent and identically distributed (i.i.d.) zero-mean circularly-symmetric complex Gaussian (ZMCSCG). Note that the rich-scattering assumption is critical to ensure Eve is not able to glean information during the SKG process and arrive at a good estimate of the key herself, since experimental studies have shown that, in an environment with insufficient reflections, signals received at the Ex during the channel estimation phase can be highly correlated with the main channel [18]. In this chapter we assume that the Ex is sufficiently distant from both Tx and Rx that it undergoes independent fading; effects of spatial correlation are studied in, for example, [11, 12].

For fair comparison of different antenna configurations, we normalize the channel entries $[\mathbf{H}]_{i,j} \sim \mathcal{CN}(0,1)$ such that the average received SNR is independent of number of transmit antennas. The Tx communicates using a set of constellation points $\mathcal{S}$ that approximates a Gaussian input scheme. The Tx and Rx begin by estimating the channel and agreeing on a secret key $\mathbf{k} \triangleq [k_1\ k_2\ \ldots\ k_{d_a}]^{\mathrm{T}}$, with $k_i \in \mathcal{S}$. The Ex is

assumed sufficiently distant from both Tx and Rx such that its probability of guessing the key is no better than chance. Define d_a, d_b, and d_c as the respective number of OTP, unencrypted and AN symbols transmitted, and the set $D \triangleq \{d_a, d_b, d_c\}$.

Let $\mathbf{a} \triangleq [a_1 \ a_2 \ \dots \ a_{d_a}]^{\mathrm{T}}$, with $a_i \in \mathcal{S}$, be the symbol vector to be encrypted with key $\mathbf{k}$. Define $\mathbf{b} \triangleq [b_1 \ b_2 \ \dots \ b_{d_b}]^{\mathrm{T}}$ and $\mathbf{c} \triangleq [c_1 \ c_2 \ \dots \ c_{d_c}]^{\mathrm{T}}$ as vectors of unencrypted and AN symbols, respectively. Alice has t degrees of freedom in designing her transmit vector, at least e of which must be devoted to interfering with Eve, and at most r of which can transmit information to Bob. Formally, the requirements on D are

R1. $d_a + d_b + d_c \leq t$

R2. $0 < d_a + d_b \leq r$

R3. $d_a + d_c \geq e$.

Note that the first inequality in R2 avoids the trivial cases where no information symbols are transmitted, while R1 ensures that Bob is able to decode all information symbols sent. The justification for R3 follows the main results.

Define an encryption function $f_e : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$ and decrypting function $f_d : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$, and let the perfectly encrypted OTP vector be $\breve{\mathbf{a}} = [\breve{a}_1 \ \breve{a}_2 \ \dots \ \breve{a}_{d_s}]^{\mathrm{T}}$, where $\breve{a}_i = f_e(a_i, k_i)$. The OTP key $\mathbf{k}$ ensures a one-to-one mapping from symbol to encrypted symbol given the key symbol, i.e. $f_d(f_e(a_i, k_i), k_i) = a_i$. Moreover, since the k_i are uniformly distributed over $\mathcal{S}$, it also ensures no information is leaked to anyone intercepting the encrypted symbol, i.e. $I(f_e(a_i, k_i); a_i) = 0$. Therefore, we have the two following properties:

$$h(\mathbf{a}|\breve{\mathbf{a}}, \mathbf{k}) = 0 \tag{135}$$

$$h(\mathbf{a}|\breve{\mathbf{a}}) = h(\mathbf{a}). \tag{136}$$

Using R1-3, the Tx forms the message and AN symbol vector as $\underline{\mathbf{s}} \triangleq \underline{\breve{\mathbf{a}}} + \underline{\mathbf{b}} + \underline{\mathbf{c}}$,

where

$$\underline{\mathbf{a}} = \left[\mathbf{a}^{\mathrm{T}}\ \mathbf{0}_{t-d_a}^{\mathrm{T}}\right]^{\mathrm{T}} \tag{137}$$

$$\underline{\check{\mathbf{a}}} = \left[\check{\mathbf{a}}^{\mathrm{T}}\ \mathbf{0}_{t-d_a}^{\mathrm{T}}\right]^{\mathrm{T}} \tag{138}$$

$$\underline{\mathbf{b}} = \left[\mathbf{0}_{d_a}^{\mathrm{T}}\ \mathbf{b}^{\mathrm{T}}\ \mathbf{0}_{t-d_a-d_b}^{\mathrm{T}}\right]^{\mathrm{T}} \tag{139}$$

$$\underline{\mathbf{c}} = \left[\mathbf{0}_{d_a+d_b}^{\mathrm{T}}\ \mathbf{c}^{\mathrm{T}}\ \mathbf{0}_{t-d_a-d_a-d_c}^{\mathrm{T}}\right]^{\mathrm{T}}. \tag{140}$$

Using the SVD, the Tx precodes with the right singular vectors to form transmitted vector $\mathbf{x} \triangleq \mathbf{V}\underline{\mathbf{s}}$. The received vectors for the main channel and eavesdropper channel, respectively, are then

$$\mathbf{y}_m = \mathbf{H}\mathbf{x} + \mathbf{n}_m \tag{141}$$

$$\mathbf{y}_e = \mathbf{G}\mathbf{x} + \mathbf{n}_e, \tag{142}$$

where the channel matrix entries $[\mathbf{H}]_{i,j}, [\mathbf{G}]_{i,j} \sim \mathcal{CN}(0,1)$ for all $i \in \{1,2,\ldots r\}, j \in \{1,2,\ldots t\}$, $\mathbf{n}_m \sim \mathcal{CN}(0,\sigma_{n_m}^2\mathbf{I})$, and $\mathbf{n}_e \sim \mathcal{CN}(0,\sigma_{n_e}^2\mathbf{I})$. Let the transmit covariance matrices corresponding to (137)-(140) above be $\mathbf{Q}_j \triangleq \mathbf{V}\mathrm{E}[\mathbf{j}\mathbf{j}^{\mathrm{H}}]\mathbf{V}^{\mathrm{H}}$ for $\mathbf{j} \in \{\underline{\mathbf{a}}, \underline{\check{\mathbf{a}}}, \underline{\mathbf{b}}, \underline{\mathbf{c}}\}$. Let the corresponding powers be $P_a = \mathrm{tr}(\mathbf{Q}_a) = \mathrm{tr}(\mathbf{Q}_{\check{a}})$, $P_b = \mathrm{tr}(\mathbf{Q}_b)$, and $P_c = \mathrm{tr}(\mathbf{Q}_c)$. Define the set $Q \triangleq \{\mathbf{Q}_a, \mathbf{Q}_b, \mathbf{Q}_c\}$, and let $\mathcal{Q}$ be the set of all Q fulfilling requirements R1-3 and power constraint $P_a + P_b + P_c \leq P$.

5.3 DCAN With Error-Free CSI

In this section, we make the following assumptions about CSI:

A1. Both the Tx and Rx have full, instantaneous, and error-free knowledge of the main channel matrix $\mathbf{H}$, and know the statistics of the eavesdropper channel $\mathbf{G}$ but have no knowledge of a specific realization.

A2. The Ex has full, instantaneous and error-free knowledge of the eavesdropper channel $\mathbf{G}$ and of the right singular vector matrix $\mathbf{V}$ of the main channel.

Note that in much of the existing AN literature, the worst-case scenario where the Ex has full knowledge of $\mathbf{H}$ is commonly assumed. Since the Ex is able to receive the training signals from the Tx, she may easily estimate $\mathbf{G}$. However, given sufficient scattering in the environment and spatial separation, it is likely to be overly pessimistic that the Ex could reliably know $\mathbf{H}$. Any eavesdropper's best hope of acquiring main-channel state information is to have either Tx or Rx reveal information to her. This might come in the form of feedback during the main-channel estimation process. For example, in the LTE standard, the Rx feeds back to the Tx the index of a quantized version of the precoding matrix $\mathbf{V}$ [1]. As a worst-case scenario here, we assume the Ex has perfect knowledge of $\mathbf{V}$ rather than a quantized version.

Given that we reveal $\mathbf{V}$ to the Ex, a natural question is whether or not revealing $\mathbf{V}$ might also inadvertently reveal other information about $\mathbf{H}$. This question is addressed with the following Lemma:

Lemma 1. *Let the SVD of an $n \times m$ matrix $\mathbf{B}$ with entries $[\mathbf{B}]_{i,j} \sim \mathcal{CN}(0,1)$ for all i, j be $\mathbf{B} = \mathbf{U}_B \mathbf{\Sigma}_B \mathbf{V}_B^H$. Then $\mathbf{V}_B$ and $\mathbf{U_B}$ are mutually independent, and are also individually independent of $\mathbf{\Sigma}_B$.*

Proof. Since the entries of $\mathbf{B}$ are zero-mean complex Gaussian, the columns of $\mathbf{B}$ are zero-mean complex Gaussian vectors. Therefore, the product $\mathbf{B}^{\mathrm{H}}\mathbf{B}$ is a central complex Wishart matrix, and has eigenvalue decomposition $\mathbf{V}_B \mathbf{\Lambda}_B \mathbf{V}_B^{\mathrm{H}}$, where $\mathbf{\Lambda}_B = \mathbf{U}_B^{\mathrm{H}} \mathbf{\Sigma}_B \mathbf{\Sigma}_B^{\mathrm{H}} \mathbf{U}_B^{\mathrm{H}}$. By [85, Lemma 2.6], $\mathbf{V}_B$ is a Haar matrix uniformly distributed on the set of $m \times m$ unitary matrices, and is therefore independent of $\mathbf{\Lambda}_B$. The proof is completed by noting that the product $\mathbf{B}\mathbf{B}^{\mathrm{H}}$ is also a central complex Wishart matrix, and therefore independence similarly applies to left singular matrices $\mathbf{U}_B$. □

Lemma 1 shows that revealing $\mathbf{V}$ to Eve does not risk revealing additional correlated information about the main channel. We can therefore assume that Eve has full knowledge of $\mathbf{V}$ without compromising the information-theoretic security. Given this

model, with requirements R1-3 and assumptions A1-2, we present the main results of this chapter in the following theorem:

Theorem 1. *In a MIMOME wiretap channel, fix the realization of main and eavesdropper channels as* $\mathbf{H}$ *and* $\mathbf{G}$*, respectively. Then, for any chosen transmit covariance matrices set* Q*, the secrecy rate using the DCAN scheme is*

$$R_s^Q(\mathbf{H},\mathbf{G},Q) = \left[\log_2 \frac{|\sigma_{n_m}^2\mathbf{I}_r + \mathbf{H}(\mathbf{Q}_a+\mathbf{Q}_b)\mathbf{H}^H|}{|\sigma_{n_m}^2\mathbf{I}_r|} - \log_2 \frac{|\sigma_{n_e}^2\mathbf{I}_e + \mathbf{G}(\mathbf{Q}_{\check{a}}+\mathbf{Q}_b+\mathbf{Q}_c)\mathbf{G}^H|}{|\sigma_{n_e}^2\mathbf{I}_e + \mathbf{G}(\mathbf{Q}_{\check{a}}+\mathbf{Q}_c)\mathbf{G}^H|}\right]^+, \tag{143}$$

and the maximum is taken over the set $\mathcal{Q}$ *as*

$$R_s^{\mathrm{DCAN}}(\mathbf{H},\mathbf{G}) = \max_{Q\in\mathcal{Q}} R_s^Q(\mathbf{H},\mathbf{G},Q). \tag{144}$$

Proof. The upper bound on achievable secrecy rates in a Gaussian MIMO wiretap channel is defined as the difference in mutual information between the main and eavesdropper channels [7] given channels $\mathbf{H}$ and $\mathbf{G}$. For DCAN, we assume that the main channel mutual information is also conditioned on the given realization of secret key $\mathbf{k}$. Let the SVD of the fixed main channel be $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{\mathrm{H}}$. The achievable secrecy rates with DCAN are upper bounded by

$$R_s^{\mathrm{DCAN}} = \max_{p(\mathbf{x})} [I(\mathbf{a},\mathbf{b};\mathbf{y}_m|\mathbf{H}=\mathbf{H},\mathbf{k}) - I(\mathbf{a},\mathbf{b};\mathbf{y}_e|\mathbf{G},\mathbf{V})]^+, \tag{145}$$

where $p(\mathbf{x})$ is the distribution on transmitted vector $\mathbf{x}$. The first and second terms in (145) correspond to the main-channel and eavesdropper-channel rates, respectively. The first term in (145) can be written

$$I(\mathbf{a},\mathbf{b};\mathbf{y}_m|\mathbf{H},\mathbf{k}) = h(\mathbf{y}_m|\mathbf{H},\mathbf{k}) - h(\mathbf{y}_m|\mathbf{a},\mathbf{b},\mathbf{H},\mathbf{k}) \tag{146}$$

$$\overset{(a)}{=} \log_2|\pi e\mathbf{Q}_{\mathbf{y}_m|\mathbf{H},\mathbf{k}}| - \log_2|\pi e\sigma_{n_m}^2\mathbf{I}|, \tag{147}$$

where $\mathbf{Q}_{\mathbf{y}_m|\mathbf{H},\mathbf{k}} = \mathrm{E}[\mathbf{y}_m\mathbf{y}_m^{\mathrm{H}}|\mathbf{H},\mathbf{k}]$, and (a) is achieved by choosing $\mathbf{a},\mathbf{b}$ Gaussian. Since the output of the encryption function f_e is uniformly distributed over $\mathcal{S}$, we have that

$\mathrm{E}[\check{\mathbf{a}}\mathbf{b}^{\mathrm{H}}] = \mathbf{0}_{d_a \times d_b}$, and thus

$$\begin{aligned}
&\mathrm{E}[\mathbf{y}_m \mathbf{y}_m^{\mathrm{H}} | \mathbf{H}, \mathbf{k}] \\
&\quad = \mathbf{H}\mathbf{V}\mathrm{E}[\tilde{\check{\mathbf{a}}}\tilde{\check{\mathbf{a}}}^{\mathrm{H}} | \mathbf{k}]\mathbf{V}^{\mathrm{H}}\mathbf{H}^{\mathrm{H}} + \mathbf{H}\mathbf{Q}_b\mathbf{H}^{\mathrm{H}} + \sigma_{n_m}^2 \mathbf{I}_r \qquad (148) \\
&\quad = \mathbf{H}\mathbf{Q}_a\mathbf{H}^{\mathrm{H}} + \mathbf{H}\mathbf{Q}_b\mathbf{H}^{\mathrm{H}} + \sigma_{n_m}^2 \mathbf{I}_r. \qquad (149)
\end{aligned}$$

Combining the log terms, we arrive at the first term in (143). The second term in (145) can be written

$$\begin{aligned}
I(\mathbf{a}, \mathbf{b}; \mathbf{y}_e | \mathbf{G}, \mathbf{V}) &= h(\mathbf{y}_e | \mathbf{G}, \mathbf{V}) - h(\mathbf{y}_e | \mathbf{a}, \mathbf{b}, \mathbf{G}, \mathbf{V}) \\
&\overset{(b)}{=} \log_2 |\pi e \mathbf{Q}_{\mathbf{y}_e|\mathbf{G},\mathbf{V}}| - \log_2 |\pi e \mathbf{Q}_{\mathbf{y}_e|\mathbf{a},\mathbf{b},\mathbf{G},\mathbf{V}}| \\
&\overset{(c)}{=} \log_2 |\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_{\check{a}} + \mathbf{Q}_b + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}| \\
&\qquad - \log_2 |\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_{\check{a}} + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|, \qquad (150)
\end{aligned}$$

where (b) is achieved by designing $\check{\mathbf{a}}, \mathbf{b}$ and $\mathbf{c}$ (approximately) Gaussian, $\mathbf{Q}_{\mathbf{y}_e|\mathbf{G},\mathbf{V}} = \mathrm{E}[\mathbf{y}_e \mathbf{y}_e^{\mathrm{H}} | \mathbf{G}, \mathbf{V}]$, and $\mathbf{Q}_{\mathbf{y}_e|\mathbf{a},\mathbf{b},\mathbf{G},\mathbf{V}} = \mathrm{E}[\mathbf{y}_e \mathbf{y}_e^{\mathrm{H}} | \mathbf{a}, \mathbf{b}, \mathbf{G}, \mathbf{V}]$, and (c) follows from (136). Combining the log terms, the proof is complete. □

Corollary 1. *In a MIMOME wiretap channel with random main channel* $\mathbf{H}$*, random eavesdropper channel* $\mathbf{G}$*, and power constraint* P*, the maximum ergodic DCAN secrecy rate is*

$$\bar{R}_s^{\mathrm{DCAN}} = \mathrm{E}_{\mathbf{H},\mathbf{G}} \left[R_s^{\mathrm{DCAN}}(\mathbf{H}, \mathbf{G}) \right]. \qquad (151)$$

Let $\mathcal{Q}^*$ be a subset of $\mathcal{Q}$ with the additional constraints that $P_a = 0$ and $d_a = 0$. We can then define the strictly AN approach as a special case of the DCAN scheme. For comparison with previous works, we introduce the following definition:

Definition 1. [22] *In a MIMOME wiretap channel with random main channel* $\mathbf{H}$*, random eavesdropper channel* $\mathbf{G}$*, and power constraint* P*, the maximum ergodic AN secrecy rate is*

$$\bar{R}_s^{\mathrm{AN}} = \mathrm{E}_{\mathbf{H},\mathbf{G}} \left[\max_{Q \in \mathcal{Q}^*} R_s^Q(\mathbf{H}, \mathbf{G}, Q) \right], \qquad (152)$$

and the minimum secrecy rate guaranteed to be achievable with arbitrarily high eavesdropper SNR is

$$\bar{R}_s^{*\mathrm{AN}} = \lim_{\sigma_{n_e}^2 \to 0} \bar{R}_s^{\mathrm{AN}} \tag{153}$$

As SNR at the Ex grows large, the determinant in the denominator of the second term in (1) is no longer regularized by the noise term. It is noted in [22] that, to ensure a nonzero determinant, the product $\mathbf{G}\mathbf{Q}_c\mathbf{G}^{\mathrm{H}}$ be full rank. Thus in the AN-only case, we have the requirement that $d_c \geq e$. For the DCAN scheme, we have that $\mathbf{G}(\mathbf{Q}_a + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}$ must be full rank, leading to requirement R3. Clearly, with DCAN, thwarting Eve requires less degrees of freedom devoted to AN, and more degrees of freedom can then be used to transmit information. It follows that, in comparison to the strictly AN case, the DCAN scheme may allow for higher secure data rates or reduced power expenditure. To show the possible increase in rates over the AN-only case, we introduce the second Theorem using the following Lemma:

Lemma 2. *For any positive-semidefinite matrices* $\mathbf{A}$ *and* $\mathbf{B}$ *with arbitrary but identical dimension* $n \times n$*,*

$$|\mathbf{A} + \mathbf{B}| \geq |\mathbf{A}|. \tag{154}$$

Proof. See Appendix 5.7.1. □

Threorem 2. *In a MIMOME wiretap channel with random main channel* $\mathbf{H}$*, random eavesdropper channel* $\mathbf{G}$*, and power constraint* P*, the maximum ergodic DCAN secrecy rate* $\bar{R}_s^{\mathrm{DCAN}}$ *is bounded by*

$$\bar{R}_s^{\mathrm{AN}} \leq \bar{R}_s^{\mathrm{DCAN}} \leq \bar{C}, \tag{155}$$

where the upper bound is achieved when $d_a = r$*, the lower bound is achieved when* $d_a = 0$*, where*

$$\bar{C} = \mathrm{E}_{\mathbf{H}}\left[\max_{Q \in \mathcal{Q}} \log_2 \left| \mathbf{I}_r + \frac{1}{\sigma_{n_m}^2} \mathbf{H}(\mathbf{Q}_a + \mathbf{Q}_b)\mathbf{H}^{\mathrm{H}} \right| \right] \tag{156}$$

is the ergodic capacity of the main channel assuming full channel state information at the transmitter and receiver.

Proof. We first prove the right hand side of (155). Since all product terms inside determinants in (143) are positive semidefinite, by Lemma 2 we have that

$$|\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_{\check{a}} + \mathbf{Q}_b + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}| \geq |\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_{\check{a}} + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|, \tag{157}$$

and hence that

$$\log_2 \frac{|\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_{\check{a}} + \mathbf{Q}_b + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|}{|\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_{\check{a}} + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|} \geq 0. \tag{158}$$

Since $\mathbf{Q}_b$ is a covariance matrix, any nonzero $\mathbf{Q}_b$ will result in the left hand side of (158) nonzero, and therefore will yield a rate strictly less than (156). To establish the equality condition, note that $\bar{R}_s^{\mathrm{DCAN}} = \bar{C}$ implies (158) is fulfilled with equality. Then it must be that $\mathbf{Q}_b = \mathbf{0}$, which implies that $d_b = 0$ and $P_b = 0$. Thus achieving the ergodic capacity is possible only by setting $\mathbf{Q}_b$ to $\mathbf{0}$ in (156) and allocating power to $\mathbf{Q}_{\check{a}}$ according to the standard waterfilling solution. Since ergodic capacity is achieved using all receive antennas, we conclude that $d_a = r$.

Next we prove the left hand side of (155). The equality condition is straightforward by removing the possibility of encrypted symbols, i.e. $d_a = 0$ and $P_a = 0$. This is the aforementioned subset $\mathcal{Q}^*$ which leads to (152). To establish the inequality, note that equation (144) is a maximization over $\mathcal{Q}$. Since $\mathcal{Q}^*$ is a subset of $\mathcal{Q}$, any antenna configuration and power allocation yielding a rate less than (152) will be superseded by (152) in the maximization; therefore the rate maximized over a larger set can only yield a greater (or equal) value. □

Theorem 2 demonstrates the true utility of the DCAN method, since the achievable secrecy rates are at least as good as the AN-only scheme, and potentially showing rates nearing the ergodic channel capacity. The price paid for the increase in secrecy rates is additional processing in the SKG step; therefore DCAN would be best suited for systems where secrecy is of utmost importance, even at the expense of complexity.

Definition 2. *The minimum secrecy rate guaranteed to be achievable with DCAN and with arbitrarily high eavesdropper SNR is*

$$\bar{R}_s^{*\mathrm{DCAN}} = \lim_{\sigma_{n_e}^2 \to 0} \bar{R}_s^{\mathrm{DCAN}}. \tag{159}$$

Definition 3. *For a MIMOME system employing DCAN, fix the power P^{DCAN} to meet the desired secrecy criterion. The* power savings *of the DCAN approach over an AN-only strategy with total power P^{AN} is defined as*

$$\begin{aligned} P^{\mathrm{S}} &= \min\left[P^{\mathrm{AN}}\right] - P^{\mathrm{DCAN}} \\ \text{subject to: } & \bar{R}_s^{\mathrm{AN}} \geq \bar{R}_s^{\mathrm{DCAN}}. \end{aligned} \tag{160}$$

In Section 5.5 we use Definition 2 to demonstrate that DCAN offers greater secrecy rates than AN only even in the worst case of zero eavesdropper noise, and Definition 3 to illustrate the power saved by choosing DCAN over an AN-only strategy.

5.4 DCAN With Imperfect Channel Estimation

In this section we relax the assumption that error free CSIT and CSIR are instantaneously available. Rather, the channel will be decomposed into a known, estimated part $\hat{\mathbf{H}}$ and a random error $\tilde{\mathbf{H}}$, with $\mathbf{H} = \hat{\mathbf{H}} + \tilde{\mathbf{H}}$. We assume that the legitimate receiver chooses $\hat{\mathbf{H}}$ to be the minimum mean-square error (MMSE) estimate. With Gaussian channel inputs, the MMSE estimate is also the linear minimum mean-square error (LMMSE) estimate. Since the entries of $\mathbf{H}$ are ZMCSCG, and using the fact that for LMMSE estimation the error terms are uncorrelated, the entries of $\tilde{\mathbf{H}}$ are i.i.d. and ZMCSCG with variance $\sigma_{\tilde{\mathbf{H}}}^2$.

If the statistics of the eavesdropper channel match those of the main channel, then the eavesdropper channel will also evolve during the SKG process, and the result is a slight mismatch between the actual and estimated channels at the Ex. Similar to the main channel, the actual eavesdropper decomposes additively into estimated and error terms as $\mathbf{G} = \hat{\mathbf{G}} + \tilde{\mathbf{G}}$. The entries of $\tilde{\mathbf{G}}$ are i.i.d. ZMCSCG with variance

$\sigma^2_{\tilde{\mathbf{G}}} = \sigma^2_{\tilde{\mathbf{H}}}$. However, since we are unable to guarantee any estimation fidelity criterion at the Ex, we will assume the worst case where $\sigma^2_{\tilde{\mathbf{G}}} \to 0$. Formally, we have the following modified assumptions:

A1′. Both the Tx and Rx know the estimate $\hat{\mathbf{H}}$, and know only the statistics of the estimation error $\tilde{\mathbf{H}}$ and eavesdropper channel $\mathbf{G}$.

A2′. The Ex has full, instantaneous and error-free knowledge of the eavesdropper channel $\mathbf{G}$ and of the right singular vector matrix $\hat{\mathbf{V}}$ of the estimated main channel.

It is difficult to derive expressions for the achievable rates using DCAN when the channel must be estimated. However, it is possible to derive upper and lower bounds on the mutual information between channel inputs and outputs under different assumptions [55, 100]. We assume the Tx diagonalizes the estimated main channel using SVD to minimize AN leakage caused by imperfect CSI.[2] Let the SVD of the estimated channel be $\hat{\mathbf{H}} = \hat{\mathbf{U}}\hat{\Sigma}\hat{\mathbf{V}}^{\mathrm{H}}$. Then the message and AN symbols can be precoded with $\hat{\mathbf{V}}$ to form the transmit vector $\overline{\mathbf{x}} = \hat{\mathbf{V}}\underline{\mathbf{s}}$. Define $\hat{\mathbf{V}}_a, \hat{\mathbf{V}}_b, \hat{\mathbf{V}}_{ab}$ and $\hat{\mathbf{V}}_c$ as the submatrices of $\hat{\mathbf{V}}$ with all rows and selected columns corresponding to $\check{\mathbf{a}}, \mathbf{b}, [\check{\mathbf{a}}^T \ \mathbf{b}^T]^T$ and $\mathbf{c}$, respectively. Define $\mathbf{R}_{ab} = \mathrm{diag}(\mathbf{R}_a \ \mathbf{R}_b)$. The output of the main channel is

$$\mathbf{z}_m = \mathbf{H}\overline{\mathbf{x}} + \mathbf{n}_m, \tag{161}$$

$$= (\hat{\mathbf{H}} + \tilde{\mathbf{H}})\hat{\mathbf{V}}\overline{\mathbf{x}} + \mathbf{n}_m \tag{162}$$

$$= \hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}[\check{\mathbf{a}}^T \ \mathbf{b}^T]^T + \tilde{\mathbf{H}}\overline{\mathbf{x}} + \mathbf{n}_m, \tag{163}$$

$$= \hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}[\check{\mathbf{a}}^T \ \mathbf{b}^T]^T + \mathbf{w}_m, \tag{164}$$

[2] Although not strictly optimal at low SNR [45], the SVD yields optimal precoding as number of antennas grows large and at moderate to high SNR. Even in low SNR conditions, SVD offers a low-complexity precoding approach with nearly-optimal performance

where (163) is reached by noting that the AN vector $\mathbf{c}$ reaches the output only through the channel estimation error, and where $\mathbf{w}_m = \tilde{\mathbf{H}}\overline{\mathbf{x}} + \mathbf{n}_m$ is the interference plus noise vector at the Rx. The output at the Ex becomes

$$\mathbf{z}_e = \mathbf{G}\hat{\mathbf{V}}\overline{\mathbf{x}} + \mathbf{n}_e \tag{165}$$

$$= \mathbf{G}\hat{\mathbf{V}}_b\mathbf{b} + \big(\mathbf{G}(\hat{\mathbf{V}}_a\check{\mathbf{a}} + \hat{\mathbf{V}}_c\mathbf{c}) + \mathbf{n}_e\big) \tag{166}$$

$$= \hat{\mathbf{G}}\hat{\mathbf{V}}_b\mathbf{b} + \tilde{\mathbf{G}}\hat{\mathbf{V}}\mathbf{b} + \mathbf{w}_e, \tag{167}$$

where $\mathbf{w}_e = \big(\mathbf{G}(\hat{\mathbf{V}}_a\check{\mathbf{a}} + \hat{\mathbf{V}}_c\mathbf{c}) + \mathbf{n}_e\big)$ is the interference plus noise vector at the Ex.

Threorem 3. *In a MIMOME wiretap channel with main channel estimate* $\hat{\mathbf{H}}$*, eavesdropper channel estimate* $\hat{\mathbf{G}}$*, and power constraint* P*, the maximum ergodic DCAN secrecy rate* $\bar{R}_{\tilde{s}}^{\mathrm{DCAN}}$ *is bounded by*

$$\bar{R}_{\tilde{s}}^{L} \leq \bar{R}_{\tilde{s}}^{\mathrm{DCAN}} \leq \bar{R}_{\tilde{s}}^{U}, \tag{168}$$

where

$$\bar{R}_{\tilde{s}}^{U} = \mathrm{E}\left[\log_2 \frac{\big|\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\mathbf{R}_{ab}\hat{\mathbf{V}}_{ab}^H\hat{\mathbf{H}} + (P\sigma_{\tilde{\mathbf{H}}}^2 + \sigma_{\mathbf{n}_m}^2)\mathbf{I}_r\big|}{\big|\big(\sigma_{\tilde{\mathbf{H}}}^2\|\overline{\mathbf{x}}\|^2 + \sigma_{\mathbf{n}_m}^2\big)\big(\mathbf{I}_e + \mathbf{R}_{\mathbf{w}_e}^{-1}\hat{\mathbf{G}}\hat{\mathbf{V}}_b\mathbf{R}_b(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)^H\big)\big|}\right], \tag{169}$$

and

$$\bar{R}_{\tilde{s}}^{L} = \mathrm{E}\left[\log_2 \frac{\big|\mathbf{I}_{d_a+d_b} + \mathbf{R}_{ab}(\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^H\mathbf{R}_{\mathbf{w}_m}^{-1}\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\big|}{\big|\mathbf{I}_e + \mathbf{G}\hat{\mathbf{V}}_b\mathbf{R}_b\hat{\mathbf{V}}_b^H\mathbf{G}^H\mathbf{R}_{\mathbf{w}_e}^{-1}\big|}\right]. \tag{170}$$

Proof. See Appendix 5.7.2. □

Although deriving exact closed-form expressions for the imperfect-CSI case is difficult, instead of exact expressions we may substitute use of the upper and lower bounds, so long as the bounds are tight for values of interest. We show by simulation in Section 5.5 that the derived bounds are tight for a reasonable range of estimation error.

5.5 Simulation Results

To verify the DCAN Theorems 1 and 2 presented in Section 5.2, we ran 2×10^3 Monte Carlo simulations using $(8, 4, 4)$ antennas at Alice, Bob and Eve, respectively. To measure the effects of a broad range of Eavesdropper SNR, we tested values of $SNR_e = \{0, 10, 35, 100\}$ dB. Note that the $SNR_e = 100$ dB case simulates the worst-case scenario where the Ex has attempted to maximize its SNR by moving close to the transmitter. For the case of imperfect CSI, our analysis differs fundamentally from [101, 102], where CSI for the main (MISOSE) channel is quantized to a finite number of bits, since we assume both Tx and Rx are able to estimate the main (full MIMOME) channel with sufficient accuracy to form a secret key. Rather, the imperfect CSI in our system is the result of channel evolution during the overhead time associated with the key generation process.

In Figure 30, we compare the DCAN scheme with a main-channel SNR of 20 dB to the corresponding maximum ergodic secrecy rate in the AN-only case for the same values of Ex SNR, antenna configuration and main-channel SNR. The ergodic AN-only rate in (152) is selected as the maximum achievable average, allocating signal power $m\alpha P$ and AN power $(1-m\alpha)P$, with step size $\alpha = 0.02$ and $m = \{0, 1, \ldots, 50\}$. Although it is well known that, for a MIMO channel with full CSIT, the capacity-achieving power allocation is achieved via the standard waterfilling solution (see, e.g. [24, Ch.10.7]), for DCAN the optimality of waterfilling is not clear. Also well known is the fact that as SNR increases, the waterfilling solution converges to uniform power allocation. Therefore, at high SNR uniform power allocation is chosen for its simpler implementation, while at lower SNR we compare the two methods.

The top plot in Figure 30 shows the rates achievable by using DCAN to encrypt varying numbers of transmitted symbols for the case of uniform power allocation at low (5 dB) main channel SNR. The results are shown for various eavesdropper SNRs. To benchmark the success of the scheme, these figures also show the ergodic MIMO

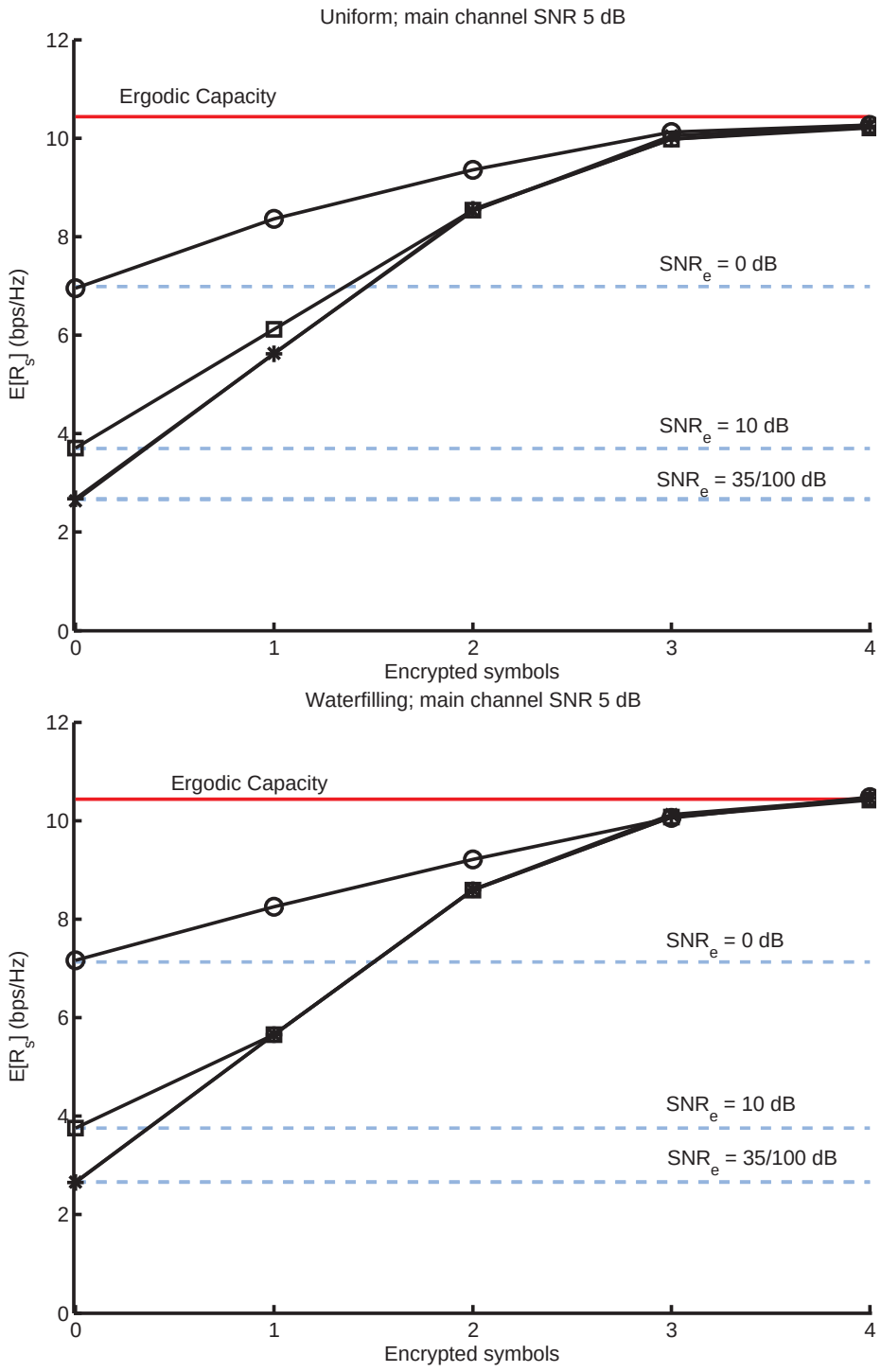


Figure 30: DCAN achievable rates (solid black lines) with uniform power allocation (top) and using waterfilling (bottom) for the low SNR case for a MIMOME system with $t = 8$, $r = 4$, and $e = 4$. Dotted blue lines denote the rates achieved by the AN-only case defined in (152); solid lines with $\{\bigcirc, \square, +, \times\}$ markers denote rates achieved with DCAN (151) with respective eavesdropper SNR of $\{0, 10, 35, 100\}$ dB.

capacity (horizontal solid line) assuming full CSIT, the same antenna configuration, and the same transmitted power, as well as rates achievable using only AN (horizontal dotted lines) for the various values of SNR_e tested. Note that the $SNR_e = 100$ line is nearly indistinguishable from $SNR_e = 35$, and thus can be a good approximation for the worst case where $SNR_e \to \infty$.

In each case, the DCAN method is shown to be identical to the AN-only case when no symbols can be encrypted. The bottom plot in Figure 30 shows the same curves for the waterfilling solution. As expected, when all symbols are encrypted (i.e. $d_a = 4$), waterfilling yields an available secrecy rate matching the ergodic capacity of the channel. The interpretation here is that the achievable secrecy is no longer dependent on the AN symbols, since each information symbol is perfectly encrypted, but rather is limited by the physical properties of the channel and the Gaussian receiver noise at the Rx. Similarly, the DCAN curves for uniform power in the top of Figure 30 show a maximum rate slightly below capacity even when all symbols are encrypted. Note that, while the rates for waterfilling and uniform power are nearly identical when $SNR_e \to \infty$, uniform power allocation can achieve slightly higher secrecy rates with moderate SNR_e and when a single symbol is encrypted.

Rates for higher (20 dB) main channel SNR, shown in Figure 31, show similar trends as the low SNR cases, and increase monotonically with each additional encrypted symbol. When power is allocated uniformly, we see that the greatest secrecy gains come invariably from the first encrypted symbol, and gains decrease monotonically thereafter. This is encouraging, since one of the primary drawbacks of generating secret keys from randomness in wireless channels is low key bit rate. Our results show that, even when bit rate is low, encrypting just one symbol can have a dramatic impact on achievable secrecy. This fact is supported on Figure 32, which show the excess power required by and AN-only system to achieve the same amount of secrecy as the DCAN scheme for high main-channel SNR. As SNR_e grows large, a single encrypted

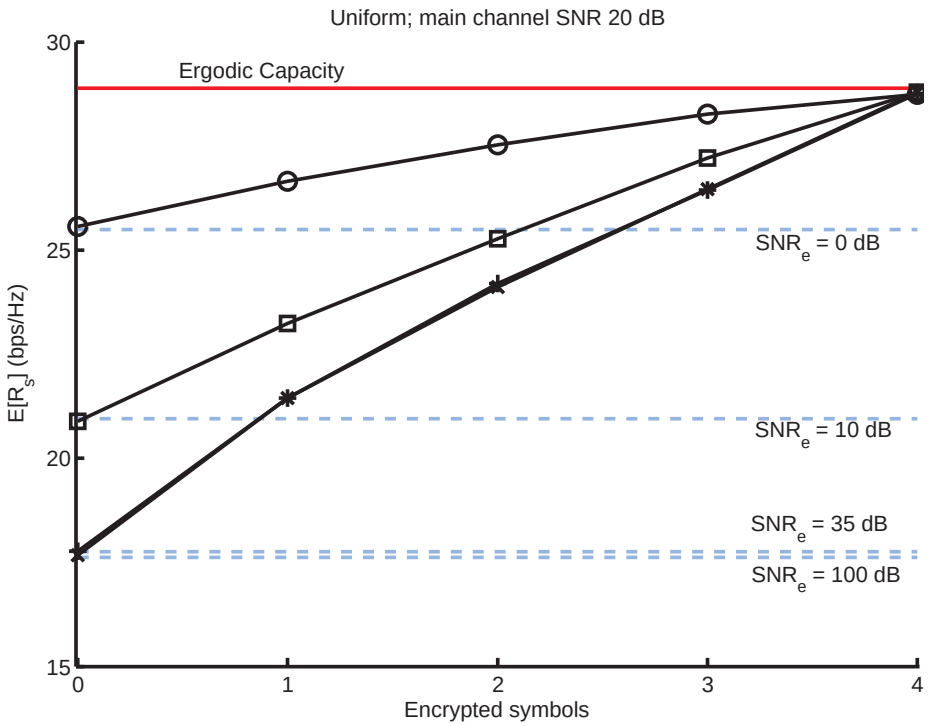


Figure 31: DCAN achievable rates in (solid black lines) with uniform power allocation for the high SNR case for a MIMOME system with $t = 8$, $r = 4$, and $e = 4$. Dotted blue lines denote the rates achieved by the AN-only case defined in (152); solid lines with $\{\bigcirc, \square, +, \times\}$ markers denote rates achieved with DCAN (151) with respective eavesdropper SNR of $\{0, 10, 35, 100\}$ dB.

symbol saves about 2.5 dB of transmitted power, and each subsequent symbol encrypted saves approximately an additional 2 dB. The low main-channel SNR case is shown on the bottom in Figure 32; it is clear that the benefit from encrypting a single symbol is even more pronounced.

Simulations for bounds on the DCAN minimum-guaranteed secrecy rate (i.e., $\sigma^2_{\mathbf{n}_e} \to 0$ and $\sigma^2_{\tilde{\mathbf{G}}} \to 0$) defined in Theorem 3 are shown in Figure 33. The three sets of bounds shown are for $\sigma^2_{\tilde{H}} = \{.001,\ .01,\ .1\}$. The solid black, solid red horizontal, and solid blue horizontal lines represent the perfect estimation case, ergodic capacity, and AN-only case for comparison. The bounds are tight for estimation errors below 0.1. As expected, the greater error values shift the overall rate down from the error-free case. For high main-channel SNR, the overall trend versus number of encrypted symbols is insensitive to amount of channel estimation error; for low SNR,

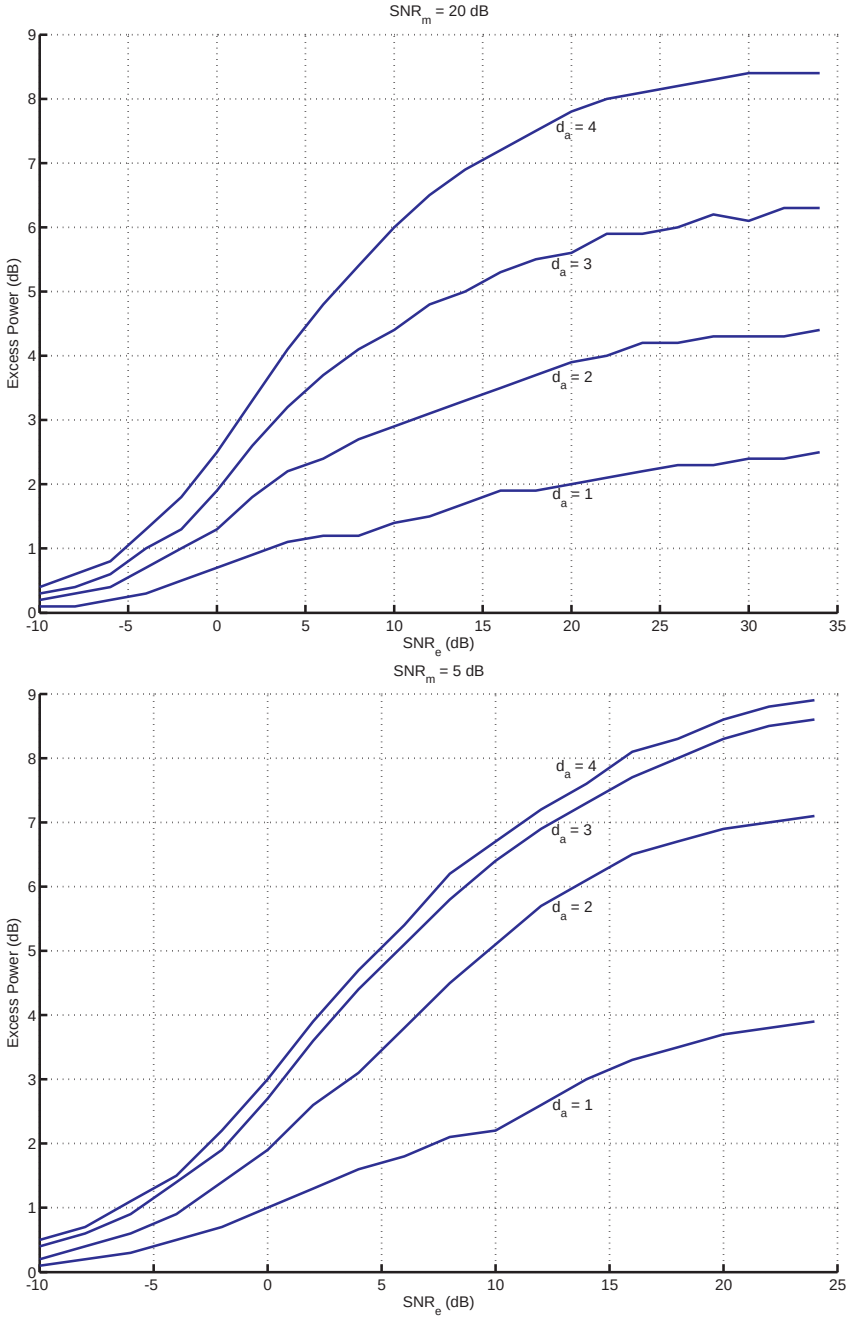


Figure 32: Excess power required for an AN-only scheme to achieve the same secrecy rate as the DCAN scheme (i.e. power saved by using DCAN), for (a) high, and (b) low, main-channel SNR with $t = 8$, $r = 4$, and $e = 4$.

however, the secrecy rate using lower numbers of encrypted symbols is less affected than the rate at higher numbers.

5.6 Discussion

We have shown how the channel estimation process common to the AN and KG techniques can be leveraged in a MIMOME wiretap channel to enhance achievable secrecy rates and save power over the AN-only scheme. We demonstrate improvements in secret communication rates using a simple uniform power allocation strategy. Our scheme relaxes the common assumption that the eavesdropper has full knowledge of the main channel fading coefficients, and instead assumes only full knowledge of the right singular vector matrix. Our results show that partially one-time padding a message prior to transmission can help protect the remaining unencrypted message, even in particular when only one message symbol is encrypted.

5.7 Appendices

5.7.1 Appendix 1

By the Minkowsky determinant theorem [56], $|\mathbf{A}+\mathbf{B}|^{1/n} \geq |\mathbf{A}|^{1/n} + |\mathbf{B}|^{1/n}$. Since $\mathbf{A}$ and $\mathbf{B}$ are positive definite, all the eigenvalues for both matrices are strictly positive. Raising to the power n and noting that the determinant of a matrix is the product of it eigenvalues, we may then discard cross terms to arrive at $|\mathbf{A}+\mathbf{B}| \geq |\mathbf{A}| + |\mathbf{B}|$. Noting again the positive-semidefiniteness of $\mathbf{B}$, it follows that $|\mathbf{A}| + |\mathbf{B}| \geq |\mathbf{A}|$, and hence $|\mathbf{A}+\mathbf{B}| \geq |\mathbf{A}|$.

5.7.2 Appendix 2

To prove Theorem 3, we first derive upper and lower bounds for the main and eavesdropper channels separately. The average mutual information of the main channel given the MMSE estimate can be written

$$I(\mathbf{a},\mathbf{b};\mathbf{z}_m|\hat{\mathbf{H}}) = h(\mathbf{z}_m|\hat{\mathbf{H}}) - h(\mathbf{z}_m|\mathbf{a},\mathbf{b},\hat{\mathbf{H}}). \tag{171}$$

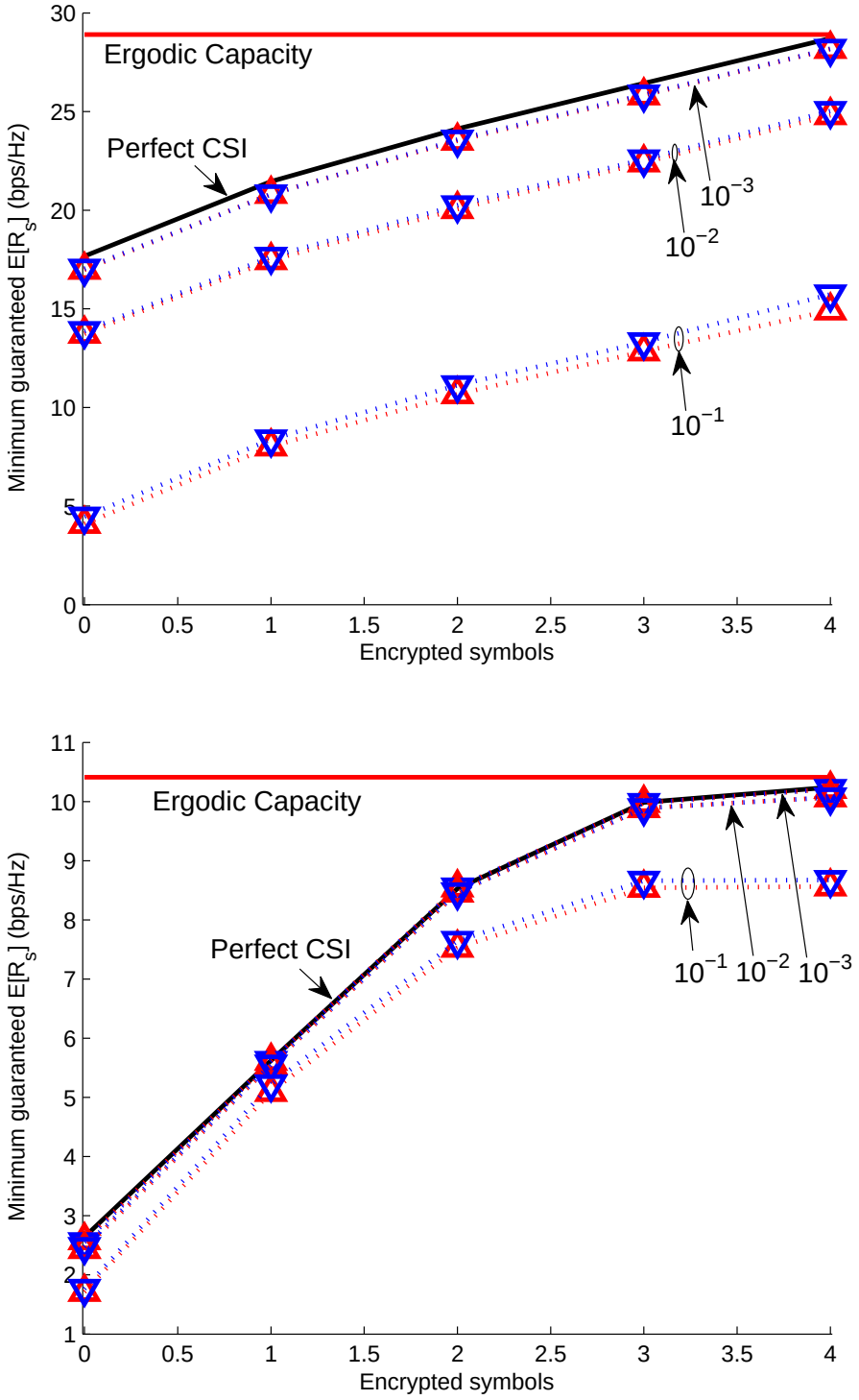


Figure 33: Bounds on the DCAN minimum achievable secrecy rate, for (a) high, and (b) low, main-channel SNR with $t = 8$, $r = 4$, and $e = 4$. The three sets of bounds shown are for $\sigma^2_{\tilde{H}} = \{.001,\ .01,\ .1\}$. Curves with red "up" arrow markers indicate the lower bound, and curves with blue "down" markers indicate the upper bound. The limiting case where $\sigma^2_{\tilde{H}} \to 0$ is given by the black curve. The upper horizontal line shows the ergodic capacity, while the lower horizontal line shows the AN-only case.

The first term in (171) can then be written

$$h(\mathbf{z}_m|\hat{\mathbf{H}}) \leq \mathrm{E}\big[\log_2|\pi e\big(\hat{\mathbf{H}}(\hat{\mathbf{V}}_a\mathbf{R}_a\hat{\mathbf{V}}_a^{\mathrm{H}} + \hat{\mathbf{V}}_b\mathbf{R}_b\hat{\mathbf{V}}_b^{\mathrm{H}})\hat{\mathbf{H}}^{\mathrm{H}} + \mathbf{R}_{\mathbf{w}_m}|\big], \tag{172}$$

where $\mathbf{R}_{\mathbf{w}_m} = \mathrm{E}[(\tilde{\mathbf{H}}\overline{\mathbf{x}} + \mathbf{n}_m)(\tilde{\mathbf{H}}\overline{\mathbf{x}} + \mathbf{n}_m)^{\mathrm{H}}]$. Using the facts that $\tilde{\mathbf{H}}\hat{\mathbf{V}}$ is equivalent to $\tilde{\mathbf{H}}$ in distribution and that the entries of $\tilde{\mathbf{H}}$ are uncorrelated ZMCSCG, the error covariance matrix simplifies to $\mathbf{R}_{\mathbf{w}_m} = P\sigma^2_{\tilde{\mathbf{H}}}\mathbf{I}$. Since differential entropy is translation invariant, the second term in (171) can be written

$$h(\mathbf{z}_m|\mathbf{a},\mathbf{b},\hat{\mathbf{H}}) = h(\mathbf{z}_m - \hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}[\mathbf{a}^T\ \mathbf{b}^T]^T|\mathbf{a},\mathbf{b}), \tag{173}$$

and the mutual information in (171) becomes

$$\begin{aligned} &I(\mathbf{a},\mathbf{b};\mathbf{z}_m|\hat{\mathbf{H}}) \\ &\quad\leq \mathrm{E}\big[\log_2\big|\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\mathbf{R}_{ab}\hat{\mathbf{V}}_{ab}^{\mathrm{H}}\hat{\mathbf{H}} + (P\sigma^2_{\tilde{\mathbf{H}}} + \sigma^2_{\mathbf{n}_m})\mathbf{I}\big|\big] \\ &\quad\quad - \mathrm{E}\big[\log_2\big|\big(\sigma^2_{\tilde{\mathbf{H}}}\|\overline{\mathbf{x}}\|^2 + \sigma^2_{\mathbf{n}_m}\big)\mathbf{I}\big|\big], \end{aligned} \tag{174}$$

where expectation in (180) is with respect to $\mathbf{H}$ and $\overline{\mathbf{x}}$ for the first and second terms, respectively.

To derive a lower bound, the mutual information in (171) can equivalently written

$$I(\mathbf{a},\mathbf{b};\mathbf{z}_m|\hat{\mathbf{H}}) = h(\mathbf{a},\mathbf{b}|\hat{\mathbf{H}}) - h(\mathbf{a},\mathbf{b}|\mathbf{z}_m,\hat{\mathbf{H}}). \tag{175}$$

Noting the translation invariance of entropy, the second term in (175) can be written

$$h(\mathbf{a},\mathbf{b}|\mathbf{z}_m,\hat{\mathbf{H}}) \leq h([\mathbf{a}^T\mathbf{b}^T]^T - [\hat{\mathbf{a}}^T\hat{\mathbf{b}}^T]|\mathbf{z}_m,\hat{\mathbf{H}}) \tag{176}$$

for any estimate $[\hat{\mathbf{a}}^T\hat{\mathbf{b}}^T]^T$. It then follows that

$$\begin{aligned} h(\mathbf{a},\mathbf{b}|\mathbf{z}_m,\hat{\mathbf{H}}) & \\ &\overset{(d)}{\leq} h([\mathbf{a}^T\mathbf{b}^T]^T - [\hat{\mathbf{a}}^T\hat{\mathbf{b}}^T]|\hat{\mathbf{H}}) \\ &\overset{(e)}{\leq} \mathrm{E}\big[\log_2\big|\pi e\big(\mathrm{cov}([\mathbf{a}^T\mathbf{b}^T]^T - [\hat{\mathbf{a}}^T\hat{\mathbf{b}}^T]^T)\big)\big|\big] \\ &\overset{(f)}{=} \mathrm{E}\big[\log_2\big|\pi e((\mathbf{R}_a+\mathbf{R}_b)^{-1} \\ &\qquad + (\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_m}^{-1}\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{-1}\big|\big], \end{aligned} \tag{177}$$

where (d) follows from the fact that conditioning can only reduce entropy, (e) follows from a Gaussian distribution maximizing entropy for a given covariance, and (f) follows from using the LMMSE estimate.

Since we choose $\mathbf{a},\mathbf{b}$ to be Gaussian, the first term in (175) is $h(\mathbf{a},\mathbf{b}|\hat{\mathbf{H}}) = \mathrm{E}[\log_2|\pi e\mathbf{R}_{ab}|]$, and the main channel mutual information lower bound is

$$I(\mathbf{a},\mathbf{b};\mathbf{y}_m|\hat{\mathbf{H}}) \geq \mathrm{E}\big[\log_2\big|\mathbf{I}+\mathbf{R}_{ab}(\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_m}^{-1}\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\big|\big]. \tag{178}$$

Thus, we have that the main channel rate $\bar{R}_m$ is bounded as $\bar{R}_m^L \leq \bar{R}_m \leq \bar{R}_m^U$, where

$$\bar{R}_m^L = \mathrm{E}\big[\log_2\big|\mathbf{I}+\mathbf{R}_{ab}(\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_m}^{-1}\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\big|\big] \tag{179}$$

$$\begin{aligned} \bar{R}_m^U = &\mathrm{E}\big[\log_2\big|\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\mathbf{R}_{ab}\hat{\mathbf{V}}_{ab}^{\mathrm{H}}\hat{\mathbf{H}} + (P\sigma_{\tilde{\mathbf{H}}}^2+\sigma_{\mathbf{n}_m}^2)\mathbf{I}\big|\big] \\ &- \mathrm{E}\big[\log_2\big|\big(\sigma_{\tilde{\mathbf{H}}}^2\|\overline{\mathbf{x}}\|^2+\sigma_{\mathbf{n}_m}^2\big)\mathbf{I}\big|\big]. \end{aligned} \tag{180}$$

The lower bound on the mutual information in the eavesdropper channel can be derived by decomposing the mutual information as

$$I(\mathbf{a},\mathbf{b};\mathbf{z}_e) = h(\mathbf{a},\mathbf{b}) - h(\mathbf{a},\mathbf{b}|\mathbf{z}_e). \tag{181}$$

The second term in (181) can be written

$$\begin{aligned} h(\mathbf{a},\mathbf{b}|\mathbf{z}_e) &\overset{(g)}{=} h(\mathbf{a}|\mathbf{z}_e) + h(\mathbf{b}|\mathbf{a},\mathbf{z}_e) \\ &\overset{(h)}{=} h(\mathbf{a}) + h(\mathbf{b}|\mathbf{a},\mathbf{z}_e) \\ &\overset{(i)}{=} h(\mathbf{a}) + h(\mathbf{b}|\mathbf{z}_e) \\ &\overset{(j)}{=} h(\mathbf{a}) + h(\mathbf{b}-\hat{\mathbf{b}}|\mathbf{z}_e) \\ &\overset{(k)}{\leq} h(\mathbf{a}) + h(\mathbf{b}-\hat{\mathbf{b}}) \\ &\overset{(l)}{\leq} \log_2|\pi e\mathbf{R}_a| + \log_2|\pi e(\mathrm{cov}(\mathbf{b}-\hat{\mathbf{b}}))|, \end{aligned} \tag{182}$$

where (g) uses the chain rule for differential entropy, (h) follows from the fact that, without the key $\mathbf{k}$, $\mathbf{z}_e$ contains no information about $\mathbf{a}$, (i) follows from the independence of $\mathbf{a}$ and $\mathbf{b}$, (j) follows from the translation invariance of entropy, (k) uses the fact that conditioning can only reduce entropy, and (l) uses the facts that $\mathbf{a}$ is Gaussian and that a Gaussian distribution maximizes the entropy for a given covariance.

Since $\mathbf{a}$ is independent of $\mathbf{b}$, we have that the joint entropy in the first term in (181) can be decomposed as $h(\mathbf{a},\mathbf{b}) = h(\mathbf{a}) + h(\mathbf{b})$. Choosing $\hat{\mathbf{b}}$ to be the LMMSE estimate yields the lower bound on mutual information

$$I(\mathbf{a},\mathbf{b};\mathbf{z}_e) \geq \log_2\left|\mathbf{I}_{d_b} + \mathbf{R}_b(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)^{\mathrm{H}}\mathbf{R}^{-1}_{\tilde{\mathbf{H}}\underline{\mathbf{b}}+\mathbf{w}_e}(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)\right|, \tag{183}$$

where $\mathbf{R}_{\tilde{\mathbf{H}}\underline{\mathbf{b}}+\mathbf{w}_e} = \mathrm{E}[(\tilde{\mathbf{H}}\underline{\mathbf{b}}+\mathbf{w}_e)(\tilde{\mathbf{H}}\underline{\mathbf{b}}+\mathbf{w}_e)^{\mathrm{H}}]$.

To derive the upper bound for the eavesdropper channel, we first show that $I(\mathbf{a},\mathbf{b};\mathbf{z}_e) \leq I(\mathbf{a},\mathbf{b};\mathbf{z}_e|\mathbf{G})$. Although conditioning can only reduce entropy, no such

relationship exists for mutual information in general. In this case, we show by subtracting

$$\begin{aligned} I(\mathbf{a},\mathbf{b};\mathbf{z}_e|\mathbf{G}) - I(\mathbf{a},\mathbf{b};\mathbf{z}) &= h(\mathbf{a},\mathbf{b}|\mathbf{G}) \\ &\quad - h(\mathbf{a},\mathbf{b}|\mathbf{z}_e,\mathbf{G}) - h(\mathbf{a},\mathbf{b}) + h(\mathbf{a},\mathbf{b}|\mathbf{z}_e) \\ &\overset{(m)}{=} h(\mathbf{a},\mathbf{b}|\mathbf{z}_e) - h(\mathbf{a},\mathbf{b}|\mathbf{z}_e,\mathbf{G}) \\ &\overset{(n)}{\geq} 0, \end{aligned} \tag{184}$$

where (m) is reached noting that $\mathbf{G}$ is independent of $\mathbf{a},\mathbf{b}$, and (n) follows from the fact that conditioning can only reduce entropy.

Using (184), we have that

$$I(\mathbf{a},\mathbf{b};\mathbf{z}_e) \leq \mathrm{E}\big[h(\mathbf{z}_e|\mathbf{G}) - h(\mathbf{z}_e|\mathbf{a},\mathbf{b},\mathbf{G})\big] \tag{185}$$

$$= \mathrm{E}\big[\log_2|\mathbf{I}_e + \mathbf{G}\hat{\mathbf{V}}_b\mathbf{R}_b\hat{\mathbf{V}}_b^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_e}^{-1}|\big]. \tag{186}$$

Thus, we have that the eavesdropper channel rate $\bar{R}_e$ is bounded as $\bar{R}_e^L \leq \bar{R}_e \leq \bar{R}_e^U$, where

$$\bar{R}_e^L = \log_2\big|\mathbf{I}_{d_b} + \mathbf{R}_b(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)^{\mathrm{H}}\mathbf{R}^{-1}_{\tilde{\mathbf{H}}\underline{\mathbf{b}}+\mathbf{w}_e}(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)\big| \tag{187}$$

$$\bar{R}_e^U = \mathrm{E}\big[\log_2|\mathbf{I}_e + \mathbf{G}\hat{\mathbf{V}}_b\mathbf{R}_b\hat{\mathbf{V}}_b^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_e}^{-1}|\big]. \tag{188}$$

The proof is completed by assigning $\bar{R}_{\tilde{s}}^U = \bar{R}_m^U - \bar{R}_e^L$ and $\bar{R}_{\tilde{s}}^L = \bar{R}_m^L - \bar{R}_e^U$.

Chapter VI

CONCLUDING REMARKS

In this dissertation, we have presented tools for interference design and two new methods of design for specific wireless communication systems. Interference channels are difficult problems both computationally and analytically. However, careful design of interference can help alleviate problems that arise. When analytical solutions, or even solutions found through simulation, are over-burdensome, choosing appropriate approximations in the systems analyzed can make problems more tractable. While interference is typically though only of as something to be avoided or compensated for, we have also shown how interference can be designed and used to achieve specific goals. The specific main contributions of this dissertation are summarized below:

- We proposed a method of analyzing an ad-hoc network interference system to determine whether a message is likely to be able to cross the network given a similar network of interference nodes. When using intentional interference to disrupt a signal, jamming is an attractive choice due to its simple implementation. However, jamming is costly from a power expenditure standpoint. Ideally, interference should be designed such that the goal of message disruption is met with minimal wasted resources. We have presented a method of approximating an interference network which allows designers to determine how best to select other system parameters, such as power, number of interference nodes, or node placement.

- As a second tool in interference design, we proposed an approximation to the MIMOME artificial-noise secrecy rate using large-scale approximation. This

approximation was based on random matrix theory in the limit of a large-antenna system, and allowed calculation of achievable secrecy rates. However, even though the approximation was derived based on infinite antenna configurations, we showed it to be accurate even for reasonable finite configurations. We differentiated performance of two approximations, one for the main channel and one for the eavesdropper channel. Solutions to both channel approximations were found in closed form. We showed that the overall approximation was very accurate in mid to high SNR, and provided a speedup of many orders of magnitude over Monte Carlo simulation.

- We presented a method of designing a fully cooperative communication-radar system to eliminate interference. We used time-domain zero padding to decouple the training and data signals at the receiver, and showed that both systems were then able to use low-complexity linear processing to achieve their individual goals. We presented a new lower bound using a least-squares approach that bounds the joint system performance when prior knowledge of the channel is unavailable or inaccurate. Since necessary power levels for the radar system dwarfed those of the communication system, making real-world amplification unfeasible, we proposed a PAPR reduction method using Barker sequences to spread power over multiple training sequences. We showed that Barker sequences had almost no effect on the probability of detection, but did decrease the lower bound on capacity.

- We presented a new DCAN approach to secret communication that combines two previously studied approaches: secret key generation, and artificial noise. This new method leverages the noise-like property of secret keys to *increase* interference seen by the eavesdropper. DCAN was proven to yield secret communication rates at least as good as the artificial noise alone, and potentially

reaching ergodic capacity. The first analysis presented assumed that the overhead in the key generation process was negligible. We then presented a second analysis assuming that key generation resulted in a Gaussian channel estimation error of known variance. Upper and lower bounds on the achievable rates using DCAN were derived, and we then showed the bound to be tight for variance up to 10% of the variance of the channel.

6.1 Future Research Topics

Addressing interference in wireless communication systems will only become more important as the number of wireless devices and uses of wireless technologies continue to proliferate. There are innumerable ways to imagine interference design research topics, from developing more tools for mitigating system complexity, to developing additional methods of using interference design to achieve specific goals. Here we list two potential future directions: one that would be a natural and direct extension of the research presented in this dissertation, and one entirely new direction (hinted at in the introduction) that could potentially blossom into a major research topic of its own.

6.1.1 DCAN in Practical Wireless Systems

One key assumption made in the study of DCAN in Chapter 5 is that the noise generated is complex Gaussian. While Gaussian noise is known to maximize interference, a Gaussian distribution does not readily lend itself to a one-time pad, since continuously distributed symbols require infinite bits to describe. It is therefore of interest to develop a finite-power signaling scheme that retains maximal ability to secure communication through interference.

The I-MMSE relation, which relates the derivative of mutual information to the MMSE of a signaling scheme for a given SNR, has already been identified as a means to develop a practical finite-power artificial noise interference scheme [3, 64]. This

relation can be used to determine the effect of a finite signaling constellation on the effectiveness of the intentional interference. For example, if the Tx were to adopt a BPSK signaling scheme for the encoded symbols, the Ex could likely estimate the symbol transmitted and subtract its effect from the remaining symbols, even if no information could be gleaned from the symbol itself. Finite constellations such as 64-QAM better mimic the Gaussian distribution in terms of the MMSE [48]. However, constellations with fine resolution also require more key bits per symbol.

For wiretap channels the eavesdropper channel is by definition unknown at the transmitter or receiver. However, in broadcast channels with confidential messages, all users are within the network and therefore all channels are known, including that of the eavesdropper. Knowledge of the eavesdropper channel facilitates many analyses not possible in the wiretap channel. For example, finding the optimal power allocation becomes more feasible using the generalized singular-value decomposition (GSVD) to compute the singular values for the joint set of main and eavesdropper channels.

6.1.2 Secrecy with Blind Interference Alignment (BIA)

Designing interference to align onto a small subspace of the signal space at the intended receiver(s) in wireless communication systems has gained interest over the last decade. This technique, known as interference alignment (IA), has been shown to increase the degrees of freedom (DoF), i.e. independent signaling dimensions, available for communication beyond that possible using *orthogonal* interference mitigation techniques (i.e. code, time or frequency division). For example, in a system with K-user single-antenna pairs (referred to as the "X-Channel"), orthogonal approaches yield $1/K$ interference-free DoF per user. This is often referred to metaphorically as each user getting an equal $1/K$ slice of the total DoF "cake." In contrast, the same K-user system using IA asymptotically yields $1/2$ DoF per user, i.e. each user gets $1/2$ of the cake [8]. Previous works (e.g. [50, 31]) have also considered IA for

the symmetric MIMO X-Channel where transmitters and receivers are equipped with the same number of antennas. The extension to the general MIMO X-channel case, where transmitters and receivers have different numbers of antennas, is considered in [26].

For IA to be possible, the dimension of the total signal space must be large enough to contain both intended signal and interference in (nearly) disjoint subspaces. In a MIMO system, the necessary dimensions are provided by the antennas. This allows implementation of IA for a single instance in time. In the single-antenna case, the dimensionality of the signal space must be increased using *symbol extensions*, i.e. transmitting over multiple time instances or frequency bands. Maximum DoF are achieved by coding over an infinite number of symbol extensions, but even a finite number of symbol extensions yields greater DoF than orthogonal approaches [8]. The concept of ergodic interference alignment was presented in [59]. With ergodic alignment, blocks are coded over long intervals, and dimensionality requirements are fulfilled by the channel's continuous (commonly termed "generic" in the literature) nature. By waiting long enough, natural variations in the channel will eventually produce the necessary alignment conditions almost surely. The disadvantage to this approach, clearly, is that block lengths can grow quite long in the process.

One of the major limitations of the IA scheme is the need for *global* channel knowledge for all the users, i.e. each transmitter must have not only knowledge of its own channel, but also knowledge of the channels of *all* other users in the system. Blind interference alignment (BIA) was first presented as a solution to this major limitation in [33]. With BIA, users have no knowledge of the actual channel coefficients; rather, statistics of the channels (specifically, the coherence time and bandwidth) are assumed to be globally known. In [32], it is shown that BIA is achievable only when the users channels are selective in different ways; if one user's channel is frequency selective, the other must be time selective (and vice versa). Instead of relying on channel

fluctuations produced by the natural environment, BIA can also be achieved using antenna switching at the transmitter to generate short-term channel fluctuation [27].

The idea of BIA hinges on the assumption that the main and eavesdropper channels are *known* to be oppositely selective, i.e. if the main channel is frequency selective then the eavesdropper channel is time selective, and vice versa. This is equivalent to stating that if one channel has a short (long) coherence time, the other will have a small (large) coherence bandwidth. It was shown in [32] that using only knowledge of the channel coherence relative to the other, it is possible to align interference to lie in a small dimensional (time-frequency) subspace for each user. Using this same assumption, it is possible that a special case of BIA can be implemented to ensure privacy in a broadcast channel with confidential messages with two users of differing channel types. It is straightforward to show that each user's message would collapse onto a smaller subspace at the other user for certain channels (e.g. the 2-user MISO channel with 2 transmit and 1 receive antennas). The challenge would be to prove that such a collapse meets conditions required for a certain level of secrecy for each user.

REFERENCES

[1] 3GPP TS 36.213, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer Procedures (Release 11),"

[2] Barros, J. and Rodrigues, M., "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, pp. 356 –360, july 2006.

[3] Bashar, S., Ding, Z., and Xiao, C., "On Secrecy Rate Analysis of MIMO Wiretap Channels Driven by Finite-Alphabet Input," *IEEE Transactions on Communications*, vol. 60, pp. 3816–3825, December 2012.

[4] Bennett, C., Brassard, G., Crepeau, C., and Maurer, U., "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, pp. 1915 –1923, nov 1995.

[5] Bliss, D., "Cooperative radar and communications signaling: The estimation and information theory odd couple," in *2014 IEEE Radar Conference*, pp. 0050–0055, May 2014.

[6] Bloch, M., Barros, J., Rodrigues, M., and McLaughlin, S., "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, pp. 2515 –2534, june 2008.

[7] Bloch, M. and ao Barros, J., *Physical-Layer Security, From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[8] Cadambe, V. and Jafar, S., "Interference Alignment and Degrees of Freedom of the K-User Interference Channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 3425–3441, Aug 2008.

[9] Cavers, J., "An analysis of pilot symbol assisted modulation for rayleigh fading channels [mobile radio]," *IEEE Transactions on Vehicular Technology*, vol. 40, pp. 686–693, Nov 1991.

[10] Chebrolu, K., Raman, B., Mishra, N., Valiveti, P. K., and Kumar, R., "Brimon: A sensor network system for railway bridge monitoring," *MobiSys*, June 2008.

[11] Chen, C. and Jensen, M., "Encryption key establishment using space-time correlated MIMO channels," in *2010 IEEE Antennas and Propagation Society International Symposium (APSURSI)*, pp. 1–4, July 2010.

[12] Chen, C. and Jensen, M., "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Transactions on Mobile Computing*, vol. 10, pp. 205–215, Feb 2011.

[13] Chen, Y. and Beaulieu, N., "Optimum Pilot Symbol Assisted Modulation," *IEEE Transactions on Communications*, vol. 55, pp. 1536–1546, Aug 2007.

[14] Croft, J., Patwari, N., and Kasera, S. K., "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, pp. 70–81, ACM, 2010.

[15] Csiszár, I. and Körner, J., "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[16] Deng, H. and Himed, B., "Interference mitigation processing for spectrum-sharing between radar and wireless communications systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, pp. 1911–1919, July 2013.

[17] Donnet, B. and Longstaff, I., "Combining MIMO radar with OFDM communications," in *3rd European Radar Conference, 2006. EuRAD 2006.*, pp. 37–40, Sept 2006.

[18] Edman, M., Kiayias, A., and Yener, B., "On passive inference attacks against physical-layer key extraction?," in *Proceedings of the Fourth European Workshop on System Security*, p. 8, ACM, 2011.

[19] Etkin, R. H., Tse, D. N., and Wang, H., "Gaussian interference channel capacity to within one bit," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5534–5562, 2008.

[20] FCC Spectrum Policy Task Force, "Report of the spectrum efficiency working group," 2002.

[21] Goel, S. and Negi, R., "Secret communication in presence of colluding eavesdroppers," in *MILCOM 2005 - IEEE Military Communications Conference, 2005*, pp. 1501 –1506 Vol. 3, oct. 2005.

[22] Goel, S. and Negi, R., "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2180 –2189, June 2008.

[23] Goldsmith, A., Jafar, S., Jindal, N., and Vishwanath, S., "Capacity limits of MIMO channels," *IEEE Journal on Selected Areas in Communications*, vol. 21, pp. 684 – 702, june 2003.

[24] Goldsmith, A., *Wireless Communications*. Cambridge University Press, 2005.

[25] Golomb, S. and Scholtz, R., "Generalized Barker sequences," *IEEE Transactions on Information Theory*, vol. 11, pp. 533–537, Oct 1965.

[26] Gou, T. and Jafar, S., "Degrees of Freedom of the K User M $\times$ N MIMO Interference Channel," *IEEE Transactions on Information Theory*, vol. 56, pp. 6040–6057, Dec 2010.

[27] Gou, T., Wang, C., and Jafar, S. A., "Aiming Perfectly in the Dark-Blind Interference Alignment Through Staggered Antenna Switching," *IEEE Transactions on Signal Processing*, vol. 59, no. 6, pp. 2734–2744, 2011.

[28] Hershey, J., Hassan, A., and Yarlagadda, R., "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, pp. 3–6, Jan 1995.

[29] Huang, J. and others, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707, 2012.

[30] IEEE Std 802.15.4-2006, "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," 2006.

[31] Jafar, S. and Shamai, S., "Degrees of Freedom Region of the MIMO X Channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 151–170, Jan 2008.

[32] Jafar, S. A., "Blind Interference Alignment," *IEEE Journal of Selected Topics in Signal Processing*, vol. 6, no. 3, pp. 216–227, 2012.

[33] Jafar, S. A., "Exploiting Channel Correlations-Simple Interference Alignment Schemes With No CSIT," in *2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, pp. 1–5, IEEE, 2010.

[34] Jakes, W. C., ed., *Microwave Mobile Communications*. John Wiley & Sons Inc., 1975.

[35] Jana, S., Premnath, S. N., Clark, M., Kasera, S. K., Patwari, N., and Krishnamurthy, S. V., "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th annual international conference on Mobile computing and networking*, pp. 321–332, ACM, 2009.

[36] Johnson, J., Baker, C., Wang, H., Ye, L., and Zhang, C., "Assessing the potential for spectrum sharing between communications and radar systems in the l-band portion of the rf spectrum allocated to radar," in *2014 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, pp. 331–334, Aug 2014.

[37] Kashyap, A., Basar, T., and Srikant, R., "Correlated jamming on mimo gaussian fading channels," *IEEE Transactions on Information Theory*, vol. 50, pp. 2119–2123, September 2004.

[38] Kay, S. M., *Fundamentals Statistical Signal Processing, Volume I: Estimation Theory*. Prentice-Hall PTR, 1993.

[39] Kay, S. M., *Fundamentals Statistical Signal Processing, Volume II: Detection Theory*. Prentice-Hall PTR, 1993.

[40] Khattab, S., Mosse, D., and Melhem, R., "Jamming mitigation in multi-radio wireless networks: Reactive or proactive?," *SecureComm*, September 2008.

[41] Khisti, A. and Wornell, G. W., "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 56, pp. 3088–3104, July 2010.

[42] Leung-Yan-Cheong, S. and Hellman, M. E., "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[43] Li, M., Koutsopoulos, I., and Poovendran, R., "Optimal jamming attacks and network devense policies in wireless sensor networks," *IEEE International Conference on Computer Communications (INFOCOM)*, 2007.

[44] Liang, Y.-L., Wang, Y.-S., Chang, T.-H., Hong, Y.-W., and Chi, C.-Y., "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise," in *IEEE International Symposium on Information Theory, 2009. ISIT 2009*, pp. 2351–2355, 2009.

[45] Lin, P.-H., Lai, S.-H., Lin, S.-C., and Su, H.-J., "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1728–1740, Sep. 2013.

[46] Lin, S.-C., Chang, T.-H., Liang, Y.-L., Hong, Y., and Chi, C.-Y., "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise: The Noise Leakage Problem," *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp. 901–915, 2011.

[47] Lozano, A. and Tulino, A., "Capacity of multiple-transmit multiple-receive antenna architectures," *IEEE Transactions on Information Theory*, vol. 48, no. 12, pp. 3117–3128, 2002.

[48] Lozano, A., Tulino, A., and Verdu, S., "Optimum Power Allocation for Parallel Gaussian Channels with Arbitrary Input Distributions," *IEEE Transactions on Information Theory*, vol. 52, pp. 3033–3051, July 2006.

[49] Ma, X., Giannakis, G., and Ohno, S., "Optimal training for block transmissions over doubly selective wireless fading channels," *IEEE Transactions on Signal Processing*, vol. 51, pp. 1351–1366, May 2003.

[50] Maddah-Ali, M., Motahari, A., and Khandani, A., "Communication Over MIMO X Channels: Interference Alignment, Decomposition, and Performance Analysis," *IEEE Transactions on Information Theory*, vol. 54, pp. 3457–3470, Aug 2008.

[51] Madiseh, M., McGuire, M., Neville, S., and Shirazi, A., "Secret key extraction in ultra wideband channels for unsynchronized radios," in *6th Annual Communication Networks and Services Research Conference, 2008. CNSR 2008.*, pp. 88–95, May 2008.

[52] Martin, D. and McAdam, P., "Convolutional code performance with optimal jamming," *Conf. Rec. Int. Conf. Commun.*, vol. 4, pp. 4.3.1–4.3.7, 1980.

[53] Mathai, A., *Statistical Distributions and Models with Application, An Introduction to Geometrical Probability*, vol. 1. Gordon and Breach Science Publishers, 1999.

[54] Mathur, S., Trappe, W., Mandayam, N., Ye, C., and Reznik, A., "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 128–139, ACM, 2008.

[55] Medard, M., "The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channel," *IEEE Transactions on Information Theory*, vol. 46, pp. 933–946, May 2000.

[56] Mirsky, L., *An Introduction to Linear Algebra*. Dover Publications, reissue edition ed., Nov 2011.

[57] Moler, C., "MATLAB incorporates LAPACK," 2000.

[58] Mukherjee, A. and others, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2011.

[59] Nazer, B., Gastpar, M., Jafar, S. A., and Vishwanath, S., "Ergodic Interference Alignment," *IEEE Transactions on Information Theory*, vol. 58, no. 10, pp. 6355–6371, 2012.

[60] Ohno, S. and Giannakis, G., "Capacity maximizing MMSE-optimal pilots for wireless OFDM over frequency-selective block Rayleigh-fading channels," *IEEE Transactions on Information Theory*, vol. 50, pp. 2138–2145, Sept 2004.

[61] Otto, C., Milenkovic, A., Sanders, C., and Jovanov, E., "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of Mobile Multimedia*, vol. 1, pp. 307–326, 2006.

[62] Premnath, S. N., Jana, S., Croft, J., Gowda, P. L., Clark, M., Kasera, S. K., Patwari, N., and Krishnamurthy, S. V., "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, pp. 917–930, May 2013.

[63] Qin, H., Chen, X., Sun, Y., Zhao, M., and Wang, J., "Optimal Power Allocation for Joint Beamforming and Artificial Noise Design in Secure Wireless Communications," in *2011 IEEE International Conference on Communications Workshops (ICC)*, pp. 1–5, 2011.

[64] Qin, H., Sun, Y., Chang, T.-H., Chen, X., Chi, C.-Y., Zhao, M., and Wang, J., "Power Allocation and Time-Domain Artificial Noise Design for Wiretap OFDM with Discrete Inputs," *IEEE Transactions on Wireless Communications*, vol. 12, pp. 2717–2729, June 2013.

[65] Quist, B. and Jensen, M., "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 1211–1220, July 2013.

[66] Quist, B. and Jensen, M., "Bound on the key establishment rate for multi-antenna reciprocal electromagnetic channels," *IEEE Transactions on Antennas and Propagation*, vol. 62, pp. 1378–1385, March 2014.

[67] Rapajic, P. and Popescu, D., "Information capacity of a random signature multiple-input multiple-output channel," *IEEE Transactions on Communications*, vol. 48, no. 8, pp. 1245–1248, 2000.

[68] Richards, M. A., *Fundamentals of Radar Signal Processing*. Tata McGraw-Hill Education, 2005.

[69] Romero-Zurita, N., Ghogho, M., and McLernon, D., "Outage Probability Based Power Distribution Between Data and Artificial Noise for Physical Layer Security," *Signal Processing Letters, IEEE*, vol. 19, no. 2, pp. 71–74, 2012.

[70] Rossler, C., Ertin, E., and Moses, R., "A software defined radar system for joint communication and sensing," in *2011 IEEE Radar Conference (RADAR),*, pp. 1050–1055, May 2011.

[71] Rousseaux, O., Leus, G., and Moonen, M., "Estimation and equalization of doubly selective channels using known symbol padding," *IEEE Transactions on Signal Processing*, vol. 54, pp. 979–990, March 2006.

[72] Sayeed, A. and Perrig, A., "Secure wireless communications: Secret keys through multipath," in *IEEE International Conference on Acoustics, Speech and Signal Processing, 2008. ICASSP 2008*, pp. 3013–3016, March 2008.

[73] Scharf, L. L., *Statistical Signal Processing: Detection, Estimation, and Time Series Analysis*. Addison Wesley Publishing Co., 1991.

[74] Shamai, S. and Verdu, S., "The impact of frequency-flat fading on the spectral efficiency of CDMA," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1302–1327, 2001.

[75] Shannon, C. E., "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[76] Shannon, C. E., "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[77] Sit, Y., Sturm, C., and Zwick, T., "One-stage selective interference cancellation for the OFDM joint radar-communication system," in *The 7th German Microwave Conference (GeMiC), 2012* , pp. 1–4, March 2012.

[78] Sklar, B., *Digital Communications Fundamentals and Applications*. Prentice Hall PTR, 2nd ed., 2000.

[79] Stamatiou, K. and Proakis, J. G., "Assessing the impact of physical layer techniques on ad hoc network performance," *Physical Communication*, vol. 1, pp. 84–91, March 2008.

[80] Sturm, C. and Wiesbeck, W., "Waveform design and signal processing aspects for fusion of wireless communications and radar sensing," *Proceedings of the IEEE*, vol. 99, pp. 1236–1259, July 2011.

[81] Sturm, C., Zwick, T., and Wiesbeck, W., "An OFDM system concept for joint radar and communications operations," in *VTC Spring 2009. IEEE 69th Vehicular Technology Conference, 2009.* , pp. 1–5, April 2009.

[82] Su, H.-J. and Geraniotis, E., "Low-complexity joint channel estimation and decoding for pilot symbol-assisted modulation and multiple differential detection systems with correlated Rayleigh fading," *IEEE Transactions on Communications*, vol. 50, pp. 249–261, Feb 2002.

[83] Surender, S., Narayanan, R., and Das, C., "Performance analysis of communications & radar coexistence in a covert UWB OSA system," in *2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, pp. 1–5, Dec 2010.

[84] Tse, D. and Hanly, S., "Linear multiuser receivers: effective interference, effective bandwidth and user capacity," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 641–657, 1999.

[85] Tulino, A. and Verdu, S., *Random Matrix Theory and Wireless Comunications*. now Publishers Inc., 2004.

[86] Tulino, A., Lozano, A., and Verdu, S., "MIMO capacity with channel state information at the transmitter," in *2004 IEEE Eighth International Symposium on Spread Spectrum Techniques and Applications*, pp. 22–26, 2004.

[87] Valenti, M. and Woerner, B., "Iterative channel estimation and decoding of pilot symbol assisted turbo codes over flat-fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 19, pp. 1697–1705, Sep 2001.

[88] Verdu, S., *Multiuser detection*. Cambridge university press, 1998.

[89] Wallace, J., "Secure physical layer key generation schemes: Performance and information theoretic limits," in *2009 IEEE International Conference on Communications, ICC '09*, pp. 1–5, June 2009.

[90] Wallace, J. and Sharma, R., "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 381–392, Sept 2010.

[91] Wang, L., McGeehan, J., Williams, C., and Doufexi, A., "Application of cooperative sensing in radar-communications coexistence," *IET Communications*, vol. 2, pp. 856–868, July 2008.

[92] Wang, T. and Giannakis, G. B., "Mutual information jammer-relay games," *IEEE Transactions on Information Forensics and Security*, vol. 3, pp. 290–303, June 2003.

[93] Willis, N. J., *Bistatic Radar*. SciTech Publishing, 2005.

[94] Willis, N. J. and Griffiths, H. D., eds., *Advances in Bistatic Radar*. SciTech Publishing, 2007.

[95] Wilson, R., Tse, D., and Scholtz, R., "Channel identification: Secret sharing using reciprocity in ultrawideband channels," in *IEEE International Conference on Ultra-Wideband, 2007. ICUWB 2007*, pp. 270–275, Sept 2007.

[96] Wood, A. D., Stankovic, J. A., and Zhou, G., "Deejam: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," *Proc. of SECON '07*, 2007.

[97] Wyner, A. D., "The Wire-Tap Channel," *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, 1975.

[98] Yang, X. and Swindlehurst, A., "On the Use of Artificial Interference for Secrecy with Imperfect CSI," in *2011 IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 476–480, 2011.

[99] Ye, C., Reznik, A., and Shah, Y., "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE International Symposium on Information Theory*, pp. 2593–2597, July 2006.

[100] Yoo, T. and Goldsmith, A., "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2203–2214, 2006.

[101] Zhang, X., McKay, M., Zhou, X., and Heath, R., "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 2742–2754, May 2015.

[102] Zhang, X., Zhou, X., McKay, M. R., and Heath, R. W., "Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3968–3972, IEEE, 2014.

[103] Zhang, X., Zhou, X., and McKay, M., "On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, 2013.

[104] Zhao, Q. and Swami, A., "A survey of dynamic spectrum access: Signal processing and networking perspectives," in *IEEE International Conference on Acoustics, Speech and Signal Processing, 2007. ICASSP 2007.*, vol. 4, pp. IV–1349–IV–1352, April 2007.

[105] Zhou, X. and McKay, M., "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 3831 –3842, oct. 2010.

[106] Zhu, J., Mo, J., and Tao, M., "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Communications Letters*, vol. 14, pp. 885–887, October 2010.